IOWA STATE
TEACHERS COLLEGE
SEP 11 1958
LIBRARY

AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

EDITED BY

WEI-LIANG CHOW
THE JOHNS HOPKINS UNIVERSITY

J. A. DIEUDONNÉ
NORTHWESTERN UNIVERSITY

A. M. GLEASON
HARVARD UNIVERSITY

PHILIP HARTMAN
THE JOHNS HOPKINS UNIVERSITY

WITH THE COÖPERATION OF

L. V. AHLFORS
A. BOREL
H. CARTAN
S. S. CHERN
C. CHEVALLEY
K. IWASAWA
K. KODAIRA
F. I. MAUTNER
J. MILNOR
A. WEIL

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXX, Number 3
JULY, 1958

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

PAGE

Spherical functions on a semisimple Lie group, II. By HARISH-CHANDRA, 553

On nilalgebras and linear varieties of nilpotent matrices, I. By MURRAY GERSTENHABER, ... 614

On the structure of local homeomorphisms of Euclidean n-space, II. By SHLOMO STERNBERG, ... 623

On the Pontryagin classes of certain $\boldsymbol{SO}(n)$-bundles over manifolds. By MICHEL A. KERVAIRE, ... 632

On the λ-variant of Mertens' μ-hypothesis. By AUREL WINTNER, . 639

Partitions of large bipartites. By E. M. WRIGHT, ... 643

Principal homogeneous spaces over Abelian varieties. By SERGE LANG and JOHN TATE, ... 659

Extensions of vector groups by Abelian varieties. By MAXWELL ROSENLICHT, ... 685

Quelques propriétés des variétés abéliennes en caractéristique p. par JEAN-PIERRE SERRE, ... 715

Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VIII). By JEAN DIEUDONNÉ, ... 740

On some invariants of cyclotomic fields. By KENKICHI IWASAWA, . 773

On a theorem of Torelli. By T. MATSUSAKA, ... 784

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is $8.50 in the U. S.; $8.75 in Canada; and $9.00 in other foreign countries. The price of single numbers is $2.50.

Manuscripts intended for publication in the JOURNAL should be sent to Professor W. L. CHOW, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

THE JOHNS HOPKINS PRESS supplies to the authors 100 free reprints of every article appearing in the AMERICAN JOURNAL OF MATHEMATICS. On the other hand, neither THE JOHNS HOPKINS PRESS nor the AMERICAN JOURNAL OF MATHEMATICS can accept orders for additional reprints. Authors interested in securing more than 100 reprints are advised to make arrangements directly with the printers, J. H. FURST CO., 20 HOPKINS PLACE, BALTIMORE 1, MARYLAND.

The typescripts submitted can be in English, French, German or Italian and should be prepared in accordance with the instructions listed on the inside back cover of this issue.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

SPHERICAL FUNCTIONS ON A SEMISIMPLE LIE GROUP II.*

By HARISH-CHANDRA.[1]

---

1. Introduction. Define G and K as in [2(i), § 1] and let $I_2(G)$ be the Hilbert space of all square-integrable spherical functions on G. Our main problem is to give an explicit "expansion" of a function f in $I_2(G)$, in terms of the elementary spherical functions. We shall construct a subspace $I_0(G)$ of $I_2(G)$ and give the required expansion for elements in $I_0(G)$. It seems likely that $I_0(G)$ is actually dense in $I_2(G)$. If this could be proved, our problem would be solved completely.

We have seen in [2(i), § 1] that a certain class of elementary spherical functions are parameterized by the space E/W. Fix a point λ in E. Then in [2(i)], we have studied the asymptotic behaviour of ϕ_λ on[2] $A_\mathfrak{p}$ at points which are far away from the singular[3] set. In this paper we shall consider the singular points as well. The main object here is to show that $\phi_\lambda(x)$ goes to zero very fast as x approaches infinity on G (see Theorem 2 of Section 12). Now let $d\lambda$ denote the Euclidean measure on E and put

$$\phi_a'(x) = \int_E \pi(\lambda) a(\lambda) \phi_\lambda(x)\, d\lambda \qquad (x \in G, a \in C_c^\infty(E)),$$

where π has the same meaning as in [2(i), § 3]. Let $I_0'(G)$ stand for the space of all such functions ϕ_a'. Then we shall prove that for $f \in I_0'(G)$, the integral

$$\tilde{f}(\lambda) = \int_G f(x) \phi_\lambda(x^{-1})\, dx \qquad (\lambda \in E)$$

is well defined and, in fact, it is possible to normalize dx in such a way that[2]

$$\int_G |f(x)|^2\, dx = \int_E |\tilde{f}(\lambda)|^2\, |\boldsymbol{c}(\lambda)|^{-2}\, d\lambda$$

for all f in $I_0'(G)$. In order to extend this formula to functions on $I_2(G)$,

---

* Received July 16, 1957.

[1] John Simon Guggenheim fellow.

[2] As far as possible we keep to the notation of [2(i)]. Hence any symbol which is not explicitly defined afresh should be given the same meaning as in [2(i)].

[3] We recall that a point $h \in A_\mathfrak{p}$ is called singular if $\Delta(h) = 0$.

one would have to show that $I_0'(G)$ is dense in $I_2(G)$. This however still remains to be done.

The central idea of this paper can be described as follows. We give a method of reducing questions about spherical functions on G to similar questions on a proper subgroup of G. This process enables us to use induction. Again, it is the detailed consideration of certain differential equations on G, which permits us to effect this reduction. Since we are primarily interested in the asymptotic behaviour of the corresponding solutions, we have to undertake a study of the asymptotic behaviour of the coefficients of these equations. This is done in Sections 2 to 5. Lemma 17 and its corollary bring these equations into a manageable form and we then obtain (in Section 6) some rather rough estimates concerning the behaviour of the corresponding solutions at infinity. These, in turn, enable us to prove certain results on convergence in Sections 7 and 8 and to simplify the equations by replacing them by their asymptotic form (see Lemma 24). It is this step which brings about the reduction of the problem from G to a proper subgroup (see Lemmas 27, 30 and 35).

Now we combine the above reduction with induction and first use it to make a detailed study of the function $\boldsymbol{c}$ in Section 9. In particular, we show that $|\boldsymbol{c}(s\lambda)| = |\boldsymbol{c}(\lambda)|$ for $s \in W$ and $\boldsymbol{c}^{-1}$ is analytic on E. The same method is then applied in Sections 11 and 12 to study ϕ_λ and ϕ_a' ($\lambda \in E$, $a \in C_c^\infty(E)$). The main results are contained in Theorems 1, 2 and 3.

In Section 13 we show that the mapping $a \to \int \phi_a'(x)\phi_\lambda(x^{-1})\,dx$ ($a \in C_c^\infty(E)$), for a fixed $\lambda \in E$, is a distribution on E which is given by a simple formula (see the corollary of Lemma 41). However this formula involves an unknown coefficient $\boldsymbol{\beta}(\lambda)$ and the rest of the paper is devoted to establishing a relationship between $\boldsymbol{\beta}$ and $\boldsymbol{c}$. This requires a considerable amount of fresh work. First we prove an inequality (Lemma 42) in order to ensure the convergence of some integrals taken over a certain nilpotent subgroup $\bar{N}$ of G. The corollary of Lemma 43 expresses the value of these integrals in terms of the function $\boldsymbol{\beta}$. On the other hand we show in Section 15 (Theorem 4) that the same integrals can also be expressed by means of $\boldsymbol{c}$ and this gives the required connection between $\boldsymbol{\beta}$ and $\boldsymbol{c}$. However, the proof of Theorem 4 is rather long. It depends upon a detailed study of certain differential equations on the solvable group $\bar{N}A_\mathfrak{p}$.

Finally in Section 16, we state two conjectures and show how one can obtain an explicit Plancherel formula for spherical functions on G, by assuming their validity.

The principal results of this paper have been announced in a short note [2(k)].

2. The ring $\mathfrak{R}$. Define $\mathfrak{h}_{\mathfrak{p}_0}{}^+$ as in [2(i), § 9] and fix an element $H_0 \neq 0$ in[2] $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. Let $\mathfrak{m}_0$ be the centralizer of H_0 in $\mathfrak{g}_0$. Then if θ is the automorphism of $\mathfrak{g}$ given by $\theta(X+Y) = X - Y$ $(X \in \mathfrak{k}, Y \in \mathfrak{p})$, it is obvious that $\theta(\mathfrak{m}_0) = \mathfrak{m}_0$. This implies (see [2(h), Lemma 10]) that $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$. Let $\mathfrak{m}$ be the complexification of $\mathfrak{m}_0$ in $\mathfrak{g}$. We regard $\mathfrak{g}$ as a Hilbert space in the usual way [2(i), § 9] and consider the orthogonal complement $\mathfrak{q}$ of $\mathfrak{m}$ in $\mathfrak{g}$. Then $\theta(\mathfrak{q}) = \mathfrak{q}$ and $[\mathfrak{m}, \mathfrak{q}] \subset \mathfrak{q}$. Let $\mathfrak{l}$ be the centralizer of $\mathfrak{m}$ in $\mathfrak{h}_{\mathfrak{p}}$ and put $\mathfrak{l}_0 = \mathfrak{l} \cap \mathfrak{h}_{\mathfrak{p}_0}$.

As before let P denote the set of all positive roots of $\mathfrak{g}$ (with respect to $\mathfrak{h}$). Then $\alpha(H_0) \geqq 0$ for $\alpha \in P$. Let Q be the set of those $\alpha \in P$ for which $\alpha(H_0) > 0$. Put $\mathfrak{q}_+ = \sum_{\alpha \in Q} CX_\alpha$, $\mathfrak{q}_- = \sum_{\alpha \in Q} CX_{-\alpha}$ where X_α has the usual meaning (see [2(i), § 7]). Then $\mathfrak{q} = \mathfrak{q}_+ + \mathfrak{q}_-$ and $\mathfrak{m} = \mathfrak{h} + \sum_{\alpha \in P'} (CX_\alpha + CX_{-\alpha})$, P' being the complement of Q in P. It is now obvious that $[\mathfrak{m}, \mathfrak{q}_+] \subset \mathfrak{q}_+$, $[\mathfrak{m}, \mathfrak{q}_-] \subset \mathfrak{q}_-$.

Let M and M_K be the analytic subgroups of G corresponding to $\mathfrak{m}_0$ and $\mathfrak{m}_{\mathfrak{k}_0} = \mathfrak{m}_0 \cap \mathfrak{k}_0$ respectively, Put $\mathfrak{m}_{\mathfrak{p}_0} = \mathfrak{m}_0 \cap \mathfrak{p}_0$ and let $M_{\mathfrak{p}}$ be the set of all elements in M of the form $\exp Y$ $(Y \in \mathfrak{m}_{\mathfrak{p}_0})$. Also put[4]

$$\Delta_M(m) = \det(\mathrm{Ad}(m) - \mathrm{Ad}(\theta(m)))_{\mathfrak{q}_+} \qquad (m \in M)$$

where the subscript denotes restriction on $\mathfrak{q}_+$. If $m = kp$ $(k \in M_K, p \in M_{\mathfrak{p}})$, it is obvious that $\Delta_M(m) = \det(\mathrm{Ad}(k))_{\mathfrak{q}_+} \Delta_M(p)$. Let M' be the set of those points $m \in M$ where $\Delta_M(m) \neq 0$. Then it follows that $M' = M_K M' M_K$ and $(M')^{-1} = M'$. Moreover

$$\Delta_M(\exp H) = \prod_{\alpha \in Q} (e^{\alpha(H)} - e^{-\alpha(H)}) \qquad (H \in \mathfrak{h}_{\mathfrak{p}_0}).$$

Let m be an element in M'. Since $\theta(\mathfrak{q}_+) = \mathfrak{q}_-$, it is clear that $X \to \{\mathrm{Ad}(m^{-1}) - \mathrm{Ad}(\theta(m^{-1}))\}X$ $(X \in \mathfrak{q})$ is a nonsingular linear mapping of $\mathfrak{q}$. We denote its inverse by $A(m)$.

LEMMA 1. *Put* $\mathfrak{q}_{\mathfrak{k}} = \mathfrak{q} \cap \mathfrak{k}$ *and* $\mathfrak{q}_{\mathfrak{p}} = \mathfrak{q} \cap \mathfrak{p}$. *Then if* $m \in M'$, $A(m)\mathfrak{q}_{\mathfrak{k}} = \mathfrak{q}_{\mathfrak{p}}$ *and* $A(m)\mathfrak{q}_{\mathfrak{p}} = \mathfrak{q}_{\mathfrak{k}}$.

Since $\theta(\mathrm{Ad}(x)Y) = \mathrm{Ad}(\theta(x))\theta(Y)$ $(x \in G, Y \in \mathfrak{g})$, it is obvious that under the mapping $\mathrm{Ad}(x) - \mathrm{Ad}(\theta(x))$, $\mathfrak{k}$ is mapped into $\mathfrak{p}$ and $\mathfrak{p}$ into $\mathfrak{k}$. From this our assertion follows immediately.

[4] Here we have extended θ to an automorphism of G.

For any $m \in M'$, define a linear transformation $c(m)$ on $\mathfrak{q}$ by $c(m)X = \mathrm{Ad}(m^{-1})A(m)X$ $(X \in \mathfrak{q})$. Then both $\mathfrak{q}_+$ and $\mathfrak{q}_-$ are invariant under $c(m)$. Let

$$c(m)X_\alpha = \sum_{\beta \in Q} X_\beta c_{\beta\alpha}(m) \qquad (\alpha \in Q,\ c_{\beta\alpha}(m) \in C).$$

Then $c_{\beta\alpha}(m)$, regarded as a function of m, is analytic on M'. Let $\mathfrak{R}_0$ be the ring of analytic functions on M' generated[5] over C by $c_{\beta\alpha}$ $(\beta, \alpha \in Q)$. Let $k \in M_K$ and $m \in M'$. Then it is easy to verify that $c(km) = c(m)$ and $c(mk)X = \mathrm{Ad}(k^{-1})c(m)\mathrm{Ad}(k)X$ $(X \in \mathfrak{q})$. Moreover

$$\begin{aligned}\theta(c(m)X) &= \mathrm{Ad}(\theta(m^{-1}))\theta(A(m)X) = -\mathrm{Ad}\,\theta(m^{-1})A(m)\theta(X)\\ &= \theta(X) - c(m)\theta(X),\end{aligned}$$

and therefore

$$\begin{aligned}c(m)\theta(X_\alpha) &= \theta(X_\alpha) - \theta(c(m)X_\alpha)\\ &= \theta(X_\alpha) - \sum_{\beta \in Q} \theta(X_\beta)c_{\beta\alpha}(m) \qquad (\alpha \in Q).\end{aligned}$$

Hence we get the following result.

LEMMA 2. *Let k be an element in M_K and g in $\mathfrak{R}_0$. Then $g(km) = g(m)$ $(m \in M')$ and the function $m \to g(mk)$ is also in $\mathfrak{R}_0$. Moreover the matrix coefficients of $c(m)$ (with respect to any fixed base of $\mathfrak{q}$), considered as functions on M', lie in the ring $C + \mathfrak{R}_0$.*

Now for any $x \in G$, put $x^\dagger = \theta(x^{-1})$.

LEMMA 3. $(1 - \mathrm{Ad}(m^\dagger m))c(m)X = X$ *for* $X \in \mathfrak{q}$ *and* $m \in M'$.

For $c(m)X = \mathrm{Ad}(m^{-1})A(m)X$ and therefore $(1 - \mathrm{Ad}(m^\dagger m))c(m)X = (\mathrm{Ad}(m^{-1}) - \mathrm{Ad}(m^\dagger))A(m)X = X$.

Let U be any linear subspace of $\mathfrak{g}$ containing $\mathfrak{q}_+$ and let T be a linear transformation in U which leaves $\mathfrak{q}_+$ invariant. Then we set $|T|_+ = \sup \|TX\|$ where X runs over all elements in $\mathfrak{q}_+$ with $\|X\| \leqq 1$. Let M_+ be the set of those points $m \in M$ where $|\mathrm{Ad}(m^{-1})|_+ < 1$. It is obvious that $M_+ \subset M'$, $A_{\mathfrak{p}^+} \subset M_+$ *and* $M_K M_+ M_K = M_+$. Moreover if m_1, m_2 are in M_+, the same holds for $m_1 m_2$.

LEMMA 4. *Let m be an element in M_+. Then*

$$|c(m)|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^2 \{1 - |\mathrm{Ad}(m^{-1})|_+^2\}^{-1}.$$

---

[5] This means that $\mathfrak{R}_0$ consists of those functions on M' which can be written as polynomials in $c_{\beta\alpha}$ (with complex coefficients), the constant term of the polynomial being zero.

It is clear that $\mathrm{Ad}(m^\dagger)$ is the adjoint of $\mathrm{Ad}(m)$ (in the sense of Hilbert space theory). Hence $|\mathrm{Ad}(m^\dagger m)^{-1}|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^2 < 1$. Therefore since

$$(1-\mathrm{Ad}((m^\dagger m)^{-1}))c(m)X = -\mathrm{Ad}((m^\dagger m)^{-1})X \qquad (X \in \mathfrak{q}_+)$$

from Lemma 3, it is clear that

$$c(m)X = -\sum_{1 \leqq r < \infty} \mathrm{Ad}((m^\dagger m)^{-r})X.$$

Hence $|c(m)|_+ \leqq \sum_{1 \leqq r < \infty} |\mathrm{Ad}(m^{-1})|_+^{2r} = |\mathrm{Ad}(m^{-1})|_+^2 \{1-|\mathrm{Ad}(m^{-1})|_+^2\}^{-1}$.

As usual let $\mathfrak{B}$ denote the universal enveloping algebra of $\mathfrak{g}$ and consider the subalgebra $\mathfrak{M}$ of $\mathfrak{B}$ generated by $(1, \mathfrak{m})$. We can regard any element μ of $\mathfrak{M}$ as a left-invariant differential operator on M. Applying this operator to each coefficient of the matrix of $c(m)$ (corresponding to some fixed base of $\mathfrak{q}$), we get a linear transformation $c(m;\mu)$ on $\mathfrak{q}$ $(m \in M')$.

LEMMA 5. *Let μ be any element in $\mathfrak{M}$ of degree r. Then there exists a positive number a such that*

$$|c(m;\mu)|_+ \leqq a\,|\mathrm{Ad}(m^{-1})|_+^2\{1-|\mathrm{Ad}(m^{-1})|_+^2\}^{-(r+1)}$$

for all $m \in M_+$.

Let σ denote the representation of $\mathfrak{M}$ on $\mathfrak{q}_+$ defined by $\sigma(Y)X = [Y, X]$ $(Y \in \mathfrak{m}, X \in \mathfrak{q}_+)$. We shall first prove the following result.

LEMMA 6. *Let μ be an element in $\mathfrak{M}$ of degree r. Then we can select a finite number of elements $\mu_{ij} \in \mathfrak{M}$ $(1 \leqq i \leqq 5, 1 \leqq j \leqq s)$ with the following properties. μ_{3j} are of degree lower than r and*

$$(1-\mathrm{Ad}(m^\dagger m)^{-1})c(m;\mu)X = \sum_{1 \leqq j \leqq s} \sigma(\mu_{1j})\mathrm{Ad}((m^\dagger m)^{-1})\sigma(\mu_{2j})c(m;\mu_{3j})X + \sum_{1 \leqq j \leqq s} \sigma(\mu_{4j})\mathrm{Ad}((m^\dagger m)^{-1})\sigma(\mu_{5j})X$$

for all $X \in \mathfrak{q}_+$ and $m \in M'$.

If $r = 0$, our statement follows from Lemma 3. So now suppose $r \geqq 1$ and use induction. It is clearly enough to consider the case when $\mu = Y_1 Y_2 \cdots Y_r$ $(Y_i \in \mathfrak{m}_0)$. Put $\mu_0 = Y_2 \cdots Y_r$ and $m_t = m \exp tY_1$ for $m \in M$ and $t \in R$. Then if $X \in \mathfrak{q}_+$, $m \in M'$, it is obvious that

$$[(d/dt)\{(1-\mathrm{Ad}(m_t^\dagger m_t)^{-1})c(m_t;\mu_0)X\}]_{t=0}$$
$$= (1-\mathrm{Ad}(m^\dagger m)^{-1})c(m;\mu)X + \sigma(Y_1)\mathrm{Ad}(m^\dagger m)^{-1}c(m;\mu_0)X$$
$$-\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\theta(Y_1))c(m;\mu_0)X.$$

On the other hand our induction hypothesis is applicable to μ_0 and so we can choose elements $\nu_{ij} \in \mathfrak{M}$ $(1 \leqq i \leqq 5, 1 \leqq j \leqq q)$ such that the degree of ν_{3j} is lower than $r-1$ and

$$(1 - \mathrm{Ad}(m^\dagger m)^{-1})c(m;\mu_0)X = \sum_{1 \leqq j \leqq q} \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;\nu_{3j})X + \sum_{1 \leqq j \leqq q} \sigma(\nu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{5j})X$$

for $m \in M'$ and $X \in \mathfrak{q}_+$. Therefore

$$\begin{aligned}[(d/dt)\{(1 - \mathrm{Ad}(m_t^\dagger m_t)^{-1})c(m_t;\mu_0)X\}_{t=0} \\ = \sum_{1 \leqq j \leqq q} \{&-\sigma(\nu_{1j}Y_1)\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;\nu_{3j}) \\ &+ \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\theta(Y_1)\nu_{2j})c(m;\nu_{3j}) \\ &+ \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;Y_1\nu_{3j}) - \sigma(\nu_{4j}Y_1)\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{5j}) \\ &+ \sigma(\nu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\theta(Y_1)\nu_{5j})\}X.\end{aligned}$$

By equating the two expressions for

$$[(d/dt)\{(1 - \mathrm{Ad}(m_t^\dagger m_t)^{-1})c(m_t;\mu_0)X\}]_{t=0}$$

obtained above, the assertion of the lemma follows.

Now we come to the proof of Lemma 6. If $r = 0$, our statement is true in consequence of Lemma 4. Hence we may suppose that $r \geqq 1$ and use induction on r. But we know from Lemma 6 that

$$c(m;\mu)X = \sum_{1 \leqq j \leqq s} \sum_{0 \leqq k < \infty} \mathrm{Ad}(m^\dagger m)^{-k}\{\sigma(\mu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{2j})c(m;\mu_{3j})X + \sigma(\mu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{5j})X\}$$

for $X \in \mathfrak{q}_+$ and $m \in M_+$. Moreover

$$|\mathrm{Ad}(m^\dagger m)^{-k}\sigma(\mu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{2j})c(m;\mu_{3j})|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^{2(k+1)}\,|\sigma(\mu_{1j})|_+\,|\sigma(\mu_{2j})|_+\,|c(m;\mu_{3j})|_+$$

and the degree of μ_{3j} is less than r. Therefore if we apply the induction hypothesis to μ_{3j} and observe that

$$|\mathrm{Ad}(m^\dagger m)^{-k}\sigma(\mu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{5j})|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^{2(k+1)}\,|\sigma(\mu_{4j})|_+\,|\sigma(\mu_{5j})|_+,$$

the required result follows immediately.

Let $\mathfrak{R}$ be the ring of analytic functions on M' generated over C by all functions of the form $\mu c_{\alpha\beta}$ $(\mu \in \mathfrak{M}; \alpha, \beta \in Q)$. It is obvious that if $g \in \mathfrak{R}$ and $\mu \in \mathfrak{M}$, then μg is also in $\mathfrak{R}$. The following result is an immediate consequence of Lemma 5.

LEMMA 7. *Let g be an element in $\mathfrak{R}$. Then there exists a positive number a and an integer $r \geqq 1$ such that*

$$|g(m)| \leqq a\,|\mathrm{Ad}(m^{-1})|_+^2\{1 - |\mathrm{Ad}(m^{-1})|_+^2\}^{-r}$$

for all $m \in M_+$.

3. The mapping μ_0. Let q be the number of roots in Q. Since $\mathfrak{g}$ is the orthogonal sum of $\mathfrak{m}$ and $\mathfrak{q}$, $\dim \mathfrak{g} = \dim \mathfrak{m} + \dim \mathfrak{q} = \dim \mathfrak{m} + 2q$. On the other hand, the restriction of $\mathrm{ad}\,H_0$ on $\mathfrak{q}$ is obviously nonsingular and therefore it defines a linear isomorphism of $\mathfrak{q}_\mathfrak{k}$ onto $\mathfrak{q}_\mathfrak{p}$. Hence $\dim \mathfrak{q}_\mathfrak{k} = \frac{1}{2}\dim \mathfrak{q} = q$. Let $X_\alpha = Y_\alpha + Z_\alpha$ $(Y_\alpha \in \mathfrak{p}, Z_\alpha \in \mathfrak{k})$ for $\alpha \in P$. Then $\theta(X_\alpha) = -Y_\alpha + Z_\alpha$. Since $X_\alpha, \theta(X_\alpha)$ $(\alpha \in Q)$ span $\mathfrak{q}$, it follows that Z_α $(\alpha \in Q)$ span $\mathfrak{q}_\mathfrak{k}$. Therefore Z_α $(\alpha \in Q)$ must be linearly independent over C. Put $\mathfrak{m}_\mathfrak{k} = \mathfrak{m} \cap \mathfrak{k}$ and $\mathfrak{m}_\mathfrak{p} = \mathfrak{m} \cap \mathfrak{p}$.

LEMMA[6] 8. *Suppose m is an element in M'. Then $\mathfrak{g} = \mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} + \mathfrak{m}_\mathfrak{p} + \mathfrak{k}$ where the sum is direct.*

Since $\mathfrak{m}_\mathfrak{p} + \mathfrak{k} = \mathfrak{m} + \mathfrak{q}_\mathfrak{k}$ and $\dim \mathfrak{g} = \dim \mathfrak{m} + 2\dim \mathfrak{q}_\mathfrak{k}$, it would be enough to prove that $\mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} \cap (\mathfrak{m}_\mathfrak{p} + \mathfrak{k}) = \{0\}$. So let us suppose that $X \in \mathfrak{q}_\mathfrak{k}$ and $\mathrm{Ad}(m^{-1})X \in \mathfrak{m}_\mathfrak{p} + \mathfrak{k}$. Then $(\mathrm{ad}\,H_0)^2\mathrm{Ad}(m^{-1})X \in \mathfrak{k}$ and therefore

$$(\mathrm{ad}\,H_0)^2\mathrm{Ad}(m^{-1})\,X = \theta((\mathrm{ad}\,H_0)^2\mathrm{Ad}(m^{-1})X) = (\mathrm{ad}\,H_0)^2\mathrm{Ad}(m^t)X.$$

This shows that $(\mathrm{ad}\,H_0)^2(\mathrm{Ad}\,m^{-1} - \mathrm{Ad}\,m^t)X = 0$. But since $\mathrm{ad}\,H_0$ defines a nonsingular linear transformation on $\mathfrak{q}$ and since $m \in M'$, it is now clear that $X = 0$. This proves that $\mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} \cap (\mathfrak{m}_\mathfrak{p} + \mathfrak{k}) = \{0\}$.

Let $\mathfrak{X}$ be the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{k})$ and let $\mathfrak{Q}_\mathfrak{k}$ and $\mathfrak{M}_\mathfrak{p}$ be the images in $\mathfrak{B}$ of[7] $S(\mathfrak{q}_\mathfrak{k})$ and $S(\mathfrak{m}_\mathfrak{p})$ respectively under the canonical mapping (see [2(b), p. 192]) of $S(\mathfrak{g})$ into $\mathfrak{B}$. Moreover for any $x \in G$, let $b \to b^x$ $(b \in \mathfrak{B})$ denote the automorphism of $\mathfrak{B}$ which coincides with $\mathrm{Ad}(x)$ on $\mathfrak{g}$. Consider the tensor product $V = \mathfrak{Q}_\mathfrak{k} \mathbf{X} \mathfrak{M}_\mathfrak{p} \mathbf{X} \mathfrak{X}$. Then it follows from the above result and Lemma 12 of [2(b)] that for any $m \in M'$, there exists a linear isomorphism of V onto $\mathfrak{B}$ which maps $q \mathbf{X} \mu \mathbf{X} x$ on $q^{m^{-1}}\mu x$ $(q \in \mathfrak{Q}_\mathfrak{k}, \mu \in \mathfrak{M}_\mathfrak{p}, x \in \mathfrak{X})$. Hence $\mathfrak{B} = (\mathfrak{Q}_\mathfrak{k})^{m^{-1}}\mathfrak{M}_\mathfrak{p}\mathfrak{X}$. Let $\mathfrak{Q}_\mathfrak{k}'$ denote the subspace consisting of those elements in $\mathfrak{Q}_\mathfrak{k}$ whose homogeneous component (see [2(i), Footnote 21]) of degree zero is zero. Then since V is the direct sum of $\mathfrak{Q}_\mathfrak{k} \mathbf{X} \mathfrak{M}_\mathfrak{p} \mathbf{X} (\mathfrak{X}\mathfrak{k})$, $\mathfrak{Q}_\mathfrak{k}' \mathbf{X} \mathfrak{M}_\mathfrak{p} \mathbf{X} 1$ and $1 \mathbf{X} \mathfrak{M}_\mathfrak{p} \mathbf{X} 1$, the following corollary is obvious.

---

[6] Cf. [2(i), Lemma 21].

[7] Here we follow the notation introduced in [2(g), § 2].

COROLLARY. *Suppose m lies in M'. Then*

$$\mathfrak{B} = (\mathfrak{Q}_\mathfrak{k})^{m^{-1}}\mathfrak{M}_\mathfrak{p}\mathfrak{X} = \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m^{-1}}\mathfrak{M}_\mathfrak{p} + \mathfrak{M}_\mathfrak{p}$$

where the sum is direct.

For any finite set of elements $X_1, \cdots, X_d \in \mathfrak{g}$, put

$$\sigma(X_1, X_2, \cdots, X_d) = (d!)^{-1} \sum X_{i_1} X_{i_2} \cdots X_{i_d} \in \mathfrak{B},$$

where the sum is over all permutations $(i_1, \cdots, i_d)$ of $(1, 2, \cdots, d)$. Moreover let $\mathfrak{B}_d$ denote the set of all element in $\mathfrak{B}$ of degree $\leqq d$.

LEMMA 9. *Let b be a given element in $\mathfrak{B}_d$. Then we can choose μ_0 in $\mathfrak{M}_\mathfrak{p} \cap \mathfrak{B}_d$ and a finite number of elements $\mu_i \in \mathfrak{M}_\mathfrak{p} \cap \mathfrak{B}_{d-1}$, $g_i \in \mathfrak{R}_0$ $(1 \leqq i \leqq r)$ such that*

$$b - \mu_0 - \sum_{1 \leqq i \leqq r} g_i(m)\mu_i \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m^{-1}}\mathfrak{M}_\mathfrak{p}$$

for all $m \in M'$.

We shall use the induction on d. Since $\mathfrak{g} = \mathfrak{q}_\mathfrak{p} + \mathfrak{m}_\mathfrak{p} + \mathfrak{k}$, it is obviously enough to consider the case when $b = \sigma(Y_1, \cdots, Y_e)\mu$ and $Y_j \in \mathfrak{q}_\mathfrak{p}$, $\mu \in \mathfrak{M}_\mathfrak{p}$ and μ is of degree $d - e$ $(e \geqq 1)$. Now for any $Y \in \mathfrak{q}_\mathfrak{p}$ and $m \in M'$,

$$c(m)Y = \mathrm{Ad}(m^{-1})A(m)Y = \tfrac{1}{2}Y + \tfrac{1}{2}(\mathrm{Ad}(m^{-1}) + \mathrm{Ad}\,\theta(m^{-1}))A(m)Y.$$

Since $A(m)Y \in \mathfrak{q}_\mathfrak{k} \subset \mathfrak{k}$ from Lemma 1, it is clear that $c(m)Y - \frac{1}{2}Y \in \mathfrak{k}$. Put

$$U_i(m) = 2A(m)Y_i, \qquad V_i(m) = 2c(m)Y_i - Y_i \qquad (1 \leqq i \leqq e).$$

Then $U_i(m)$, $V_i(m)$ are in $\mathfrak{k}$ and $\mathrm{Ad}(m^{-1})U_i(m) = Y_i + V_i(m)$. Let $(i_1, i_2, \cdots, i_e)$ be any permutation of $(1, 2, \cdots, e)$. Then

$$\begin{aligned}(U_{i_1}(m) \cdots U_{i_e}(m))^{m^{-1}}\mu &= (Y_{i_1} + V_{i_1}(m)) \cdots (Y_{i_e} + V_{i_e}(m))\mu \\ &= (L_{i_1} + R_{i_1} - D_{i_1}) \cdots (L_{i_e} + R_{i_e} - D_{i_e})\mu \\ &\equiv (L_{i_1} - D_{i_1}) \cdots (L_{i_e} - D_{i_e})\mu \bmod \mathfrak{B}\mathfrak{k}.\end{aligned}$$

Here L_i, R_i and D_i respectively denote the linear mappings $a \to Y_i a$, $a \to aV_i(m)$ and $a \to [V_i(m), a] = V_i(m)a - aV_i(m)$ $(a \in \mathfrak{B})$ of $\mathfrak{B}$ into itself. Since $[X, a] \in \mathfrak{B}_r$ for $X \in \mathfrak{g}$ and $a \in \mathfrak{B}_r$, it follows from Lemma 2 that we can select $b_1, \cdots, b_s \in \mathfrak{B}_{d-1}$ and $g_1', \cdots, g_s' \in C + \mathfrak{R}_0$ such that

$$(\sigma(U_1(m), \cdots, U_e(m))^{m^{-1}}\mu \equiv b + \sum_{1 \leqq i \leqq s} g_i'(m)b_i \bmod \mathfrak{B}\mathfrak{k}$$

for all $m \in M'$. But $\sigma(U_1(m), \cdots, U_e(m)) \in \mathfrak{Q}_\mathfrak{k}'$ since $U_j(m) \in \mathfrak{q}_\mathfrak{k}$ and therefore

$$b \equiv -\sum_{1 \leqq i \leqq s} g_i'(m) b_i \bmod \{\mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m-1}\mathfrak{M}_\mathfrak{p}\}.$$

Our assertion now follows immediately by the induction hypothesis.

Let $\mathfrak{R}_0\mathfrak{M}_\mathfrak{p}$ denote the set of all differential operators on M' which are of the form $\sum_{1 \leqq i \leqq r} g_i\mu_i$ $(g_i \in \mathfrak{R}_0, \mu_i \in \mathfrak{M}_\mathfrak{p})$. Then the above lemma shows that for any $b \in \mathfrak{B}$, we can select $\mu_0 \in \mathfrak{M}_\mathfrak{p}$ and $\mu \in \mathfrak{R}_0\mathfrak{M}_\mathfrak{p}$, such that

$$b - \mu_0 - \mu_m \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m-1}\mathfrak{M}_\mathfrak{p}$$

for all $m \in M'$. (Here μ_m denotes, as usual, the local expression [2(d), p. 112] of μ at m.) Moreover it follows from the Corollary of Lemma 8 that the differential operator $\mu_0 + \mu$ on M' is uniquely determined by b. Now suppose $\mu_0 + \mu = \mu_0' + \mu'$ $(\mu_0' \in \mathfrak{M}_\mathfrak{p}, \mu' \in \mathfrak{R}_0\mathfrak{M}_\mathfrak{p})$. Then $\mu_0 - \mu_0' = \mu' - \mu$ and therefore $\mu_0 - \mu_0' = (\mu' - \mu)_m$ for every $m \in M'$. In particular we can take $m = \exp tH_0$ $(t > 0)$. Then if $g \in \mathfrak{R}_0$, it follows from Lemma 7 that $\lim_{t \to +\infty} g(\exp tH_0) = 0$. Therefore $\mu_0 - \mu_0' = 0$. This proves that both μ_0 and μ are uniquely determined by b. We shall denote them by $\mu_0(b)$ and $\mu(b)$ respectively.

LEMMA 10. *Let k be an element in M_K. Then $(\mu_0(b))^k = \mu_0(b^k)$ and*[8] *$\mu(b)^k = \mu(b^k)$ for $b \in \mathfrak{B}$.*

Since $b - \mu_0(b) - \mu_m(b) \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m-1}\mathfrak{M}_\mathfrak{p}$ $(m \in M')$, it follows that

$$b^k - \mu_0(b)^k - (\mu_m(b))^k \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{km-1}\mathfrak{M}_\mathfrak{p}.$$

Therefore replacing m by mk, we find that

$$b^k - \mu_0(b)^k - (\mu_{mk}(b))^k \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m-1}\mathfrak{M}_\mathfrak{p}.$$

Now $(\mu(b)^k)_m = (\mu(b)_{k^{-1}mk})^k$ from Lemma 14 of [2(d)]. But it is clear from Lemma 2 that the differential operator $\mu(b)^k$ lies in $\mathfrak{R}_0\mathfrak{M}_\mathfrak{p}$ and $\mu(b)_{k^{-1}mk} = \mu(b)_{mk}$. Therefore

$$b^k - \mu_0(b)^k - (\mu(b)^k)_m \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m-1}\mathfrak{M}_\mathfrak{p}$$

and this proves that $\mu_0(b^k) = \mu_0(b)^k$ and $\mu(b^k) = \mu(b)^k$.

Let $I_\mathfrak{g}$ be the centralizer of $\mathfrak{k}$ in $\mathfrak{B}$ and $I_\mathfrak{m}$ the centralizer of $\mathfrak{m}_\mathfrak{k}$ in $\mathfrak{M}$.

COROLLARY. *If $b \in I_\mathfrak{g}$ then $\mu_0(b) \in I_\mathfrak{m}$.*

This is obvious from Lemma 10.

[8] See [2(d), p. 118] for the definition of $\mu(b)^k$.

For any $b \in \mathfrak{B}$, define the differential operator $\delta'(b)$ on[2] $A_\mathfrak{p}'$ as in [2(i), § 5]. It is obvious that $A_\mathfrak{p}' \subset M'$.

LEMMA 11. *Let b be an element in $\mathfrak{B}$ and select $g_i \in \mathfrak{R}_0, \mu_i \in \mathfrak{M}_\mathfrak{p}$ $(1 \leqq i \leqq r)$ such that*

$$b - \mu_0(b) - \sum_{1 \leqq i \leqq r} g_i(m)\mu_i \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{l}')^{m-1}\mathfrak{M}_\mathfrak{p}$$

for all $m \in M'$. Then

$$\delta_h'(b) = \delta_h'(\mu_0(b)) + \sum_{1 \leqq i \leqq r} g_i(h)\delta_h'(\mu_i)$$

for $h \in A_\mathfrak{p}'$.

Clearly $\mathfrak{Q}_\mathfrak{l}' \subset \mathfrak{k}\mathfrak{B}$ and therefore

$$b - \mu_0(b) - \sum_{1 \leqq i \leqq r} g_i(h)\mu_i \in \mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h-1}\mathfrak{B} \qquad (h \in A_\mathfrak{p}').$$

Also $a - \delta_h'(a) \in \mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h-1}\mathfrak{B}$ for any $a \in \mathfrak{B}$. Therefore[2]

$$\delta_h'(b) - \delta_h'(\mu_0(b)) - \sum_{1 \leqq i \leqq r} g_i(h)\delta_h'(\mu_i) \in \{\mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h-1}\mathfrak{B}\} \cap \mathfrak{H}_\mathfrak{p} = \{0\}$$

from Corollary 2 to Lemma 21 of [2(i)].

4. The connection between μ_0 and γ. Define the homomorphism γ of $I_\mathfrak{g}$ onto $I(\mathfrak{h}_\mathfrak{p})$ as in Theorem 1 of [2(i)] and consider the subgroup W' consisting of those elements[2] $s \in W$ which leave H_0 fixed. Now $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$ and $\mathfrak{h}_{\mathfrak{p}_0}$ is a maximal abelian subspace of $\mathfrak{m}_{\mathfrak{p}_0}$. Therefore since $\mathfrak{m}_0$ is the centralizer of H_0 in $\mathfrak{g}_0$, it is clear that W' can also be considered as the little Weyl group[9] of $\mathfrak{m}_0$ with respect to $\mathfrak{h}_{\mathfrak{p}_0}$. Let J' be the ring of those elements in $\mathfrak{H}_\mathfrak{p}$ which are invariant under W'. Then corresponding to Theorem 1 of [2(i)], we have a homomorphism $\gamma_\mathfrak{m}$ of $I_\mathfrak{m}$ onto J'. Define the linear function σ on $\mathfrak{h}_\mathfrak{p}$ by $\sigma(H) = \frac{1}{2}\sum_{\beta \in P'} \beta(H)$ where P' is the subset of those roots in P which vanish at H_0.

LEMMA 12. $\gamma(q) = e^{\rho-\sigma}\gamma_\mathfrak{m}(\mu_0(q)) \circ e^{-(\rho-\sigma)}$ *for* $q \in I_\mathfrak{g}$.

Define $\delta(b)$ $(b \in \mathfrak{B})$ as in Lemma 26 of [2(i)]. Then it follows from Lemma 11 that $\delta_h(q) = \delta_h(\mu_0(q)) + \delta_h(\mu_h(q))$ for $h \in A_\mathfrak{p}'$. On the other hand

$$\delta(\mu_0(q)) = e^\rho\delta'(\mu_0(q)) \circ e^{-\rho} = e^{\rho-\sigma}\{e^\sigma\delta'(\mu_0(q)) \circ e^{-\sigma}\} \circ e^{-\rho+\sigma}.$$

Now put $h_t = \exp tH$ $(t \in R)$ where H is some fixed element in $\mathfrak{h}_{\mathfrak{p}_0}^+$. Then

[9] Here we are extending the notion of the little Weyl group [2(i), § 3] to reductive Lie algebras in the obvious way (see [2(d), p. 118]).

$h_t \in A_\mathfrak{p}'$ if $t > 0$. Hence if d is the degree of q it follows from Lemma 26 of [2(i)] by taking limits in the finite-dimensional space $\mathfrak{B}_d$, that

$$\operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(q) = \gamma(q), \qquad \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_{h_t}(q)) = 0.$$

(Here we have to make use of Lemma 7 and the definition of $\mu(q)$.) Therefore $\gamma(q) = \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_0(q))$. On the other hand we can apply Corollary 2 to Lemma 21 of [2(i)] to $\mathfrak{m}$ instead of $\mathfrak{g}$. Hence for any $b \in \mathfrak{M}$ and $h \in A_\mathfrak{p}'$, there exists a unique element u in $\mathfrak{H}_\mathfrak{p}$ such that $b - u \in (\mathfrak{m}_\mathfrak{f})^{k-1}\mathfrak{M} + \mathfrak{M}\mathfrak{m}_\mathfrak{f}$. But then it follows from the definition of $\delta'(b)$ that $u = \delta_h'(b)$. Now put $\delta''(b) = e^{\sigma}\delta'(b) \circ e^{-\sigma}$ and apply Lemma 26 of [2(i)] to $\mathfrak{m}$. Then it follows that $\operatorname*{Lim}_{t\to+\infty} \delta_{h_t}''(b) = \gamma_\mathfrak{m}(b)$ provided $b \in I_\mathfrak{m}$. By the Corollary of Lemma 10, this holds in particular if $b = \mu_0(q)$. But since

$$\delta(\mu_0(q)) = e^{\rho-\sigma}\delta''(\mu_0(q)) \circ e^{-\rho+\sigma},$$

it is obvious that

$$\gamma(q) = \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_0(q)) = e^{\rho-\sigma}\gamma_\mathfrak{m}(\mu_0(q)) \circ e^{-\rho+\sigma}.$$

This proves the lemma.

COROLLARY. *Suppose q_1, q_2 are two elements in $I_\mathfrak{g}$. Then*

$$\mu_0(q_1)\mu_0(q_2) \equiv \mu_0(q_2)\mu_0(q_1) \equiv \mu_0(q_1q_2) \bmod \mathfrak{M}\mathfrak{m}_\mathfrak{f}.$$

Since $\gamma(q_1q_2) = \gamma(q_1)\gamma(q_2)$, it follows from Lemma 12 that $\gamma_\mathfrak{m}$ maps $\mu_0(q_1)\mu_0(q_2)$, $\mu_0(q_2)\mu_0(q_1)$ and $\mu_0(q_1q_2)$ into the same element $\gamma(q_1)\gamma(q_2)$. The required result now follows from the fact that the kernel of $\gamma_\mathfrak{m}$ is contained in $\mathfrak{M}\mathfrak{m}_\mathfrak{f}$ (see [2(i), Theorem 1]).

5. Some consequences of Lemma 12. For any linear function λ on $\mathfrak{h}_\mathfrak{p}$, let H_λ denote the corresponding element in $\mathfrak{h}_\mathfrak{p}$ so that $\langle H, H_\lambda\rangle = \lambda(H)$ for all $H \in \mathfrak{h}_\mathfrak{p}$. Also define I and I_0 as in the beginning of Section 2.

LEMMA 13. *$\rho - \sigma$ is invariant under W' and $H_{\rho-\sigma} \in \mathrm{I}_0$.*

Let $(\operatorname{ad} H)_{\mathfrak{q}_+}$ denote the restriction of $\operatorname{ad} H$ on $\mathfrak{q}_+$ for $H \in \mathfrak{h}_\mathfrak{p}$. It is obvious that $\operatorname{sp}(\operatorname{ad} H)_{\mathfrak{q}_+} = \rho(H) - \sigma(H)$. Since W' is the little Weyl group of $\mathfrak{m}$, we can, for any given $s \in W'$, choose $k \in M_K$ such that $\operatorname{Ad}(k)H = sH$. Since $\mathfrak{q}_+$ is invariant under k, it follows that $\operatorname{sp}(\operatorname{ad} H)_{\mathfrak{q}_+} = \operatorname{sp}(\operatorname{ad}(sH))_{\mathfrak{q}_+}$ and this shows that $\rho - \sigma$ is invariant under W'. Now in order to prove that $H_{\rho-\sigma} \in \mathrm{I}_0$, it is obviously sufficient to verify that $\beta(H_{\rho-\sigma}) = 0$ for any root $\beta \in P$ for

which $\beta(H_0)=0$. Let α denote the restriction of β on $\mathfrak{h}_\mathfrak{p}$. We may assume that $\alpha\neq 0$. Consider the corresponding reflexion $s_\alpha\in W$ (see [2(i), § 3]). It is obvious that s_α lies in W' and therefore it must leave $H_{\rho-\sigma}$ fixed. Hence $\beta(H_{\rho-\sigma})=\alpha(H_{\rho-\sigma})=0$.

Let ω denote the Casimir operator of $\mathfrak{g}$ (see [2(i), § 7]). We wish to compute $\mu_0(\omega)$.

LEMMA 14. *Let $X_1,\cdots,X_q$ be an orthonormal base for $\mathfrak{m}_{\mathfrak{p}_0}$ over R. Then $\mu_0(\omega)=X_1^2+\cdots+X_q^2+2H_{\rho-\sigma}$.*

Put $\eta_0=X_1^2+\cdots+X_q^2$. It is easy to check that $\eta_0\in I_\mathfrak{m}$ and if we apply Corollary 2 of Lemma 27 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$), it follows that $\gamma_\mathfrak{m}(\eta_0)=\overline{\omega}-\langle\sigma,\sigma\rangle$. However it is obvious that

$$e^{-\rho+\sigma}\overline{\omega}\circ e^{\rho-\sigma}=\overline{\omega}+2H_{\rho-\sigma}+\langle\rho-\sigma,\rho-\sigma\rangle.$$

Therefore if $\eta=\eta_0+2H_{\rho-\sigma}-2\langle\rho-\sigma,\sigma\rangle$, it follows again by the same corollary that

$$e^{\rho-\sigma}\gamma_\mathfrak{m}(\eta)\circ e^{-\rho+\sigma}=\overline{\omega}-\langle\rho,\rho\rangle=\gamma(\omega).$$

But in view of Lemma 12, this implies that $\gamma_\mathfrak{m}(\eta-\mu_0(\omega))=0$. However $\eta-\mu_0(\omega)$ lies in $\mathfrak{M}_\mathfrak{p}\cap I_\mathfrak{m}$. Therefore it follows from [2(i), Lemma 19] that $\eta=\mu_0(\omega)$. But we have seen above that $\beta(H_{\rho-\sigma})=0$ if $\beta(H_0)=0$ $(\beta\in P)$. Therefore $\langle\rho-\sigma,\sigma\rangle=0$ and this proves our assertion.

Put $\gamma_\mathfrak{m}'(\nu)=e^{\rho-\sigma}\gamma_\mathfrak{m}(\nu)\circ e^{-\rho+\sigma}$ $(\nu\in I_\mathfrak{m})$. Since $\rho-\sigma$ is invariant under W', it is clear that $J'=\gamma_\mathfrak{m}(I_\mathfrak{m})=\gamma_\mathfrak{m}'(I_\mathfrak{m})$. Put $r=[W:W']$ and choose elements $\nu_1=1,\nu_2,\cdots,\nu_r$ in $I_\mathfrak{m}$ such that $\gamma_\mathfrak{m}'(\nu_i)$ $(1\leqq i\leqq r)$ are homogeneous and[2] $J'=\sum_{1\leqq i\leqq r}J\gamma_\mathfrak{m}'(\nu_i)$. From Lemma 8 of [2(i)] this is possible.

LEMMA 15. $I_\mathfrak{m}\subset\sum_{1\leqq i\leqq r}\nu_i\mu_0(I_\mathfrak{g})+\mathfrak{M}\mathfrak{m}_\mathfrak{k}$.

Let ν be a given element in $I_\mathfrak{m}$. Then $\gamma_\mathfrak{m}'(\nu)\in J'$ and therefore $\gamma_\mathfrak{m}'(\nu)=\sum_{1\leqq i\leqq r}\gamma(q_i)\gamma_\mathfrak{m}'(\nu_i)$ for suitable $q_i\in I_\mathfrak{g}$ since $\gamma(I_\mathfrak{g})=J$. But $\gamma(q_i)=\gamma_\mathfrak{m}'(\mu_0(q_i))$ from Lemma 12 and therefore $\gamma_\mathfrak{m}'(\nu-\sum_{1\leqq i\leqq r}\nu_i\mu_0(q_i))=0$. However the kernels of $\gamma_\mathfrak{m}$ and $\gamma_\mathfrak{m}'$ are the same and so by applying Theorem 1 of [2(i)] to $\mathfrak{m}$, we conclude that $\nu-\sum_i\nu_i\mu_0(q_i)\in\mathfrak{M}\mathfrak{m}_\mathfrak{k}$. This proves the lemma.

COROLLARY. *Suppose $\sum_{1\leqq i\leqq r}\nu_i\mu_0(q_i)\in\mathfrak{M}\mathfrak{m}_\mathfrak{k}$ for some $q_i\in I_\mathfrak{g}$. Then $q_i\in\mathfrak{Z}$ $1\leqq i\leqq r$.*

Put $\nu=\sum_i\nu_i\mu_0(q_i)$. Then $\nu\in I_\mathfrak{m}\cap(\mathfrak{M}\mathfrak{m}_\mathfrak{k})$ and therefore $\gamma_\mathfrak{m}(\nu)=0$.

This implies that $\gamma_{\mathfrak{m}}'(v) = \sum_i \gamma_{\mathfrak{m}}'(v_i)\gamma(q_i) = 0$. But $\gamma_{\mathfrak{m}}'(v_i)$ $1 \leqq i \leqq r$ are linearly independent over $C(J)$ (see [2(i), Lemma 8]) and therefore $\gamma(q_i) = 0$ $1 \leqq i \leqq r$. Our assertion now follows from Theorem 1 of [2(i)].

The following lemma contains the main result of this section.

LEMMA 16. *Let v be an element in $I_{\mathfrak{m}}$ and suppose $v - \sum_{1 \leqq i \leqq r} v_i \mu_0(q_i)$ $\in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$ $(q_i \in I_{\mathfrak{g}})$. Then we can select a finite number of elements $g_j \in \mathfrak{R}$ and $\tau_j \in \mathfrak{M}$ $(1 \leqq j \leqq s)$ with the following property. If ϕ is any spherical function on G of class C^∞,*

$$\phi(m\,;v) = \sum_{1 \leqq i \leqq r} \phi(m\,;v_i q_i) + \sum_{1 \leqq j \leqq s} g_j(m)\phi(m\,;\tau_j)$$

for all $m \in M'$.

It is obvious that $\phi(m\,;v) = 0$ for $v \in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$. Therefore $\phi(m\,;v) = \sum_i \phi(m\,;v_i\mu_0(q_i))$. On the other hand since

$$q_i - \mu_0(q_i) - \mu_{\mathfrak{m}}(q_i) \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}},$$

it is clear that

$$\phi(m\,;\mu_0(q_i)) = \phi(m\,;q_i) - \phi(m\,;\mu(q_i)) \qquad (m \in M').$$

Therefore

$$\phi(m\,;v_i\mu_0(q_i)) = \phi(m\,;v_iq_i) - \phi(m\,;v_i \circ \mu(q_i))$$

and

$$\phi(m\,;v) = \sum_{1 \leqq i \leqq r} \phi(m\,;v_iq_i) - \sum_{1 \leqq i \leqq r} \phi(m\,;v_i \circ \mu(q_i)).$$

But since $\mu(q_i) \in \mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}}$, it is obvious that $\sum_i v_i \circ \mu(q_i) = -\sum_{1 \leqq j \leqq s} g_j\tau_j$ for suitable $g_j \in \mathfrak{R}$ and $\tau_j \in \mathfrak{M}$. This proves our assertion.

Let $l_0 = \dim \mathfrak{l}$ and let $\mathfrak{l}_0^+$ denote the set of those elements $H \in \mathfrak{l}_0$ for which $\alpha(H) > 0$ for every $\alpha \in Q$ (see Section 2 for the definition of Q). Then $H_0 \in \mathfrak{l}_0^+$. Select a base H_p $(1 \leqq p \leqq l_0)$ for $\mathfrak{l}_0$ over R and choose $q_{ijp} \in I_{\mathfrak{g}}$ $(1 \leqq i, j \leqq r, 1 \leqq p \leqq l_0)$ such that

$$H_p v_j \equiv \sum_{1 \leqq i \leqq r} v_i \mu_0(q_{ijp}) \bmod \mathfrak{M}\mathfrak{m}_{\mathfrak{k}} \qquad (1 \leqq j \leqq r, 1 \leqq p \leqq l_0).$$

Then q_{ijp} are unique mod $(I_{\mathfrak{g}} \cap \mathfrak{B}\mathfrak{k})$ from the Corollary to Lemma 15. Moreover

$$H_sH_pv_j \equiv \sum_{1 \leqq i \leqq r} H_sv_i\mu_0(q_{ijp}) \equiv \sum_{1 \leqq i,k \leqq r} v_k\mu_0(q_{kis})\mu_0(q_{ijp}) \bmod \mathfrak{M}\mathfrak{m}_{\mathfrak{k}},$$

since $\mu_0(q_{ijp}) \in I_{\mathfrak{m}}$. But $H_sH_p = H_pH_s$ and so we conclude from the corollaries of Lemmas 12 and 15 that

$$(1) \qquad \sum_{1 \leqq i \leqq r} (q_{kis}q_{ijp} - q_{kip}q_{ijs}) \equiv 0 \bmod \mathfrak{B}\mathfrak{k} \qquad (1 \leqq k, j \leqq r\,;\, 1 \leqq p, s \leqq l_0).$$

Moreover from Lemma 16, we can select a positive integer N and elements $g_{pja} \in \mathfrak{R}$, $\tau_{pja} \in \mathfrak{M}$ $(1 \leqq p \leqq l_0, 1 \leqq j \leqq r, 1 \leqq a \leqq N)$ such that

$$(2) \qquad \phi(m; H_p v_j) = \sum_{1 \leqq i \leqq r} \phi(m; v_i q_{ijp}) + \sum_{1 \leqq a \leqq N} g_{pja}(m) \phi(m; \tau_{pja}) \qquad (m \in M')$$

for any spherical function ϕ on G of class C^∞ $(1 \leqq j \leqq r, 1 \leqq p \leqq l_0)$.

6. Some rough estimates. Let $\mathfrak{F}$ be the space of all linear functions on $\mathfrak{h}_\mathfrak{p}$. For any $\lambda \in \mathfrak{F}$, put

$$\phi_\lambda(x) = \phi(\lambda : x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) - \rho(H(xk))\}dk \qquad (x \in G)$$

in the notation of Lemma 3 of [2(i)]. For $m \in M$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$ we write

$$\Phi_j(\lambda : m : H) = e^{\rho(H)} \phi(\lambda : m \exp H ; v_j) \qquad (1 \leqq j \leqq r)$$

and

$$\Psi_{pj}(\lambda : m : H) = e^{\rho(H)} \sum_{1 \leqq a \leqq N} g_{pja}(m \exp H) \phi(\lambda : m \exp H ; \tau_{pja}) \qquad (1 \leqq j \leqq r, 1 \leqq p \leqq l_0)$$

where g_{pja} and τ_{jpa} have the same meaning as in equation (2) of Section 5 and m, H are so chosen that $m \exp H \in M'$. Now let $\Phi(\lambda : m : H)$ and $\Psi_p(\lambda : m : H)$ denote the corresponding one-column matrices and define the $r \times r$ matrices $\Xi_p(\lambda)$ $(1 \leqq p \leqq l_0)$ by $\Xi_{pij}(\lambda) = \gamma(q_{jip} : (-1)^{\frac{1}{2}}\lambda)$ $(1 \leqq i, j \leqq r)$. Then it follows from equation (1) that $\Xi_p(\lambda)$ $(1 \leqq p \leqq l_0)$ commute with each other. For any $H' \in \mathfrak{l}$, put

$$\Psi_{H'}(\lambda : m : H) = \sum_p c_p \Psi_p(\lambda : m : H), \qquad \Xi(\lambda : H') = \sum_p c_p \Xi_p(\lambda) + \rho(H') I$$

where $H' = \sum_p c_p H_p$ $(c_p \in C)$ and I is the unit matrix. If $m \in M_+$ and $H \in \mathfrak{l}_0^+$, it is obvious that $m \exp tH \in M_+$ for all $t \geqq 0$. Therefore from Lemma 18 of [2(i)] and equation (2), we find that

$$d\Phi(\lambda : m : tH)/dt = \Xi(\lambda : H)\Phi(\lambda : m : tH) + \Psi_H(\lambda : m : tH) \qquad (t \geqq 0).$$

The following lemma is now obvious.

LEMMA 17.

$$d\Phi(\lambda : m ; \eta : tH)/dt = \Xi(\lambda : H)\Phi(\lambda : m ; \eta : tH) + \Psi_H(\lambda : m ; \eta : tH)$$

for $\lambda \in \mathfrak{F}$, $m \in M_+$, $H \in \mathfrak{l}_0^+$, $\eta \in \mathfrak{M}$ *and* $t \geqq 0$.

Now put $\Phi^0(\lambda:m:H)=\exp(-\Xi(\lambda:H))\Phi(\lambda:m:H)$ and

$$\Psi_{H'}{}^0(\lambda:m:H)=\exp(-\Xi(\lambda:H))\Psi_{H'}(\lambda:m:H) \qquad (H'\in \mathfrak{l}).$$

COROLLARY. *$d\Phi^0(\lambda:m;\eta:tH)/dt=\Psi_H{}^0(\lambda:m;\eta:tH)$ under the conditions of Lemma 17.*

This is an immediate consequence of the above lemma.

For any $p\times q$ matrix $u=(u_{ij})$ with complex coefficients, put $\|u\|=\{\sum_{i,j}|u_{ij}|^2\}^{\frac{1}{2}}$. We now intend to obtain an estimate for $\|\Psi_H{}^0(\lambda:m;\eta:tH)\|$. It follows from Lemma 46 of [2(i)] and Lemma 7 that for any fixed η, we can choose an integer $k\geqq 0$ and a positive number a' such that [2]

$$\|\Psi_p(\lambda:m;\eta:H)\|$$
$$\leqq a'(1+\|\lambda\|)^k\,|\operatorname{Ad}(h^{-1}m^{-1})|_+^{\,2}\{1-|\operatorname{Ad}(h^{-1}m^{-1})|_+^{\,2}\}^{-(k+1)}e^{\rho(H)}\phi((-1)^{\frac{1}{2}}\lambda_I:mh)$$

for $m\in M_+$, $H\in \mathfrak{l}_0^+$, $\lambda\in\mathfrak{F}$ and $1\leqq p\leqq l_0$. (Here $h=\exp H$.) Now put $\beta(H)=\min_{\alpha\in Q}\alpha(H)$ and $A_{\mathfrak{l}}{}^+=\exp\mathfrak{l}_0{}^+$. Then

$$|\operatorname{Ad}(h^{-1}m^{-1})|_+\leqq|\operatorname{Ad}(m^{-1})|_+e^{-\beta(\log h)}\leqq e^{-\beta(\log h)}$$

for $m\in M_+$ and $h\in A_{\mathfrak{l}}{}^+$. Hence we get the following result immediately.

LEMMA 18. *For any $\eta\in\mathfrak{M}$, we can choose an integer $k\geqq 0$ and a positive number a such that*

$$\|\Psi_H(\lambda:mh;\eta:tH)\|$$
$$\leqq a(1+\|\lambda\|)^k\,\|H\|\exp\{t\rho(H)-t\beta(H)-\beta(\log h)\}\phi((-1)^{\frac{1}{2}}\lambda_I:mh\exp tH)$$

for $\lambda\in\mathfrak{F}$, $m\in M_+$, $h\in A_{\mathfrak{l}}{}^+$, $H\in\mathfrak{l}_0{}^+$ and $t\in R$ provided $t\beta(H)+\beta(\log h)\geqq 1$.

On the other hand

$$\|\Psi_H{}^0(\lambda:m;\eta:tH)\|\leqq\|\exp(-t\Xi(\lambda:H))\|\,\|\Psi_H(\lambda:m;\eta:tH)\|.$$

So now we have to estimate $\|\exp(-t\Xi(\lambda:H))\|$. Put $\lambda^*=(-1)^{\frac{1}{2}}\lambda$ for $\lambda\in\mathfrak{F}$.

LEMMA 19. *Select r elements $s_1,s_2,\cdots,s_r$ in W such that $W=\bigcup_{1\leqq i\leqq r}W's_i$. Then if T is an indeterminate and I the $r\times r$ unit matrix,*

$$\det(TI-\Xi(\lambda:H))=\prod_{1\leqq i\leqq r}(T-\lambda^*(s_iH))$$

for $\lambda\in\mathfrak{F}$ and $H\in\mathfrak{l}$.

Fix λ and H and select $q_{ij}\in I_{\mathfrak{g}}$ $(1\leqq i,j\leqq r)$ such that $Hv_j\equiv\sum_i\nu_i\mu_0(q_{ij})$

$\bmod \mathfrak{M}\mathfrak{m}_I$. Since I is contained in the center of $\mathfrak{m}$, it follows by applying the homomorphism $\gamma_{\mathfrak{m}}$ to this relation that $Hv_j' = \sum_i v_i' \gamma_{\mathfrak{m}}(\mu_0(q_{ij}))$ where $v_i' = \gamma_{\mathfrak{m}}(v_i)$. Moreover $e^{\rho-\sigma} H \circ e^{-\rho+\sigma} = H - \rho(H)$ since σ is zero on I. So if $v_i = e^{\rho-\sigma} v_i' \circ e^{-\rho+\sigma}$, it follows from Lemma 12 that $Hv_j = \rho(H) v_j + \sum_i v_i \gamma(q_{ij})$. Now if we recall the definition of the matrix $\Xi(\lambda : H)$ and denote its coefficients by ξ_{ij}, it becomes clear that

$$Hv_j \equiv \sum_i \xi_{ji} v_i \bmod J' J_\lambda .$$

in the notation of Lemma 13 of [2(i)]. But it follows from our definition of $v_1, \cdots, v_r$ and this lemma that $v_1, \cdots, v_r$ are linearly independent $\bmod J' J_\lambda$. Hence our assertion is an immediate consequence of the corollary of Lemma 15 of [2(i)].

COROLLARY. *There exists a positive number a and an integer $k \geqq 0$ such that*

$$\| \exp(t\Xi(\lambda : H)) \| \leqq a(1 + \| \lambda \|)^k (1 + |t|)^r (1 + \| H \|)^r \times \exp\{2r |t| \max_{1 \leqq i \leqq r} |\lambda_I(s_i H)|\}$$

for $H \in \mathfrak{l}_0$, $t \in R$, and $\lambda \in \mathfrak{F}$.

It follows from the definition of $\Xi(\lambda : H)$ that we can choose a positive number b and an integer $d \geqq 0$ such that

$$\| \Xi(\lambda : H) \| \leqq b(1 + \| \lambda \|)^d \| H \| \qquad (\lambda \in \mathfrak{F}, H \in \mathfrak{l}).$$

Moreover it follows from the above lemma and [2(i), Lemma 60] that

$$\| \exp(t\Xi(\lambda : H)) \| \leqq r^{\frac{1}{2}} \exp(2r |t| \max_{1 \leqq i \leqq r} |\lambda_I(s_i H)|) \sum_{0 \leqq k \leqq r} |t|^k \| \Xi(\lambda : H) \|^k .$$

Therefore the statement of the corollary is now obvious.

For a positive number ϵ, let $\mathfrak{F}_\epsilon$ denote the set of all $\lambda \in \mathfrak{F}$ such that $\| \lambda_I \| < \epsilon$.

LEMMA 20. *Let V be a compact set in $\mathfrak{l}_0^+$. Then there exists a positive number ϵ with the following property. Let η be an element in $\mathfrak{M}$. Then we can choose an integer $k \geqq 0$ and, for any compact set ω in M_+, positive numbers a_1, a_2 and t_0 such that*

$$\| \Psi_H^0(\lambda : mh ; \eta : tH) \| \leqq a_1 (1 + \| \lambda \|)^k t^k e^{-a_2 t}$$

for $\lambda \in \mathfrak{F}_\epsilon$, $m \in \omega$, $h \in A_I^+$, $H \in V$ and $t \geqq t_0$.

Our proof depends on Lemma 18. But first we need an estimate for $\phi((-1)^{\frac{1}{2}}\lambda_I : mh)$.

LEMMA 21. *Let ϵ' be a positive number < 1. Then we can select an integer $d \geqq 0$ and positive numbers ϵ and a such that*

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh) \leqq a(1 + \| \log h \|)^d e^{-(1-\epsilon')\rho(\log h)}$$

for $m \in \omega$, $h \in A_I^+$ and $\lambda \in \mathfrak{F}_\epsilon$. Moreover d and ϵ may be so chosen that they are independent of ω.

From Theorem 3 and Lemma 49 of [2(i)], we can select d, ϵ and a positive number a' such that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : \exp H) \leqq a'(1 + \| H \|)^d e^{-(1-\epsilon')\rho(H)}$$

if $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand since ϕ_μ is a spherical function for any $\mu \in \mathfrak{F}$, it is obvious that $\phi((-1)^{\frac{1}{2}}\lambda_I : \exp H) = \phi((-1)^{\frac{1}{2}}\lambda_I : \exp sH)$ $(s \in W, H \in \mathfrak{h}_{\mathfrak{p}_0})$. Moreover $\rho(H) \geqq \rho(sH)$ for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}^+$. Therefore since $\mathfrak{h}_{\mathfrak{p}_0} = \bigcup_{s \in W} s(\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+))$ (see [2(f), Lemma 37]), we conclude that the above inequality actually holds for all $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

On the other hand $M = M_K A_{\mathfrak{p}} M_K$ (see [2(f), Lemmas 31 and 33]) and since ω is compact, we can select a positive number c such that[10] $\| \log | m | \| \leqq c$ for $m \in \omega$. For a fixed $m \in \omega$, choose $h_1 \in A_{\mathfrak{p}}$ such that $m \in M_K h_1 M_K$. Then $\| \log h_1 \| = \| \log | m | \| \leqq c$ and

$$\begin{aligned}\phi((-1)^{\frac{1}{2}}\lambda_I : mh) &= \phi((-1)^{\frac{1}{2}}\lambda_I : h_1 h) \\ &\leqq a'(1 + \| \log(h_1 h) \|)^d \exp\{-(1-\epsilon')\rho(\log(h_1 h))\}\end{aligned}$$

if $h \in A_I^+$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand we can select a positive number a'' such that

$$(1 + \| H \|)^d e^{-(1-\epsilon')\rho(H)} \leqq a''$$

for all elements $H \in \mathfrak{h}_{\mathfrak{p}_0}$ with $\| H \| \leqq c$. Then if $a = a'a''$, it follows that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh) \leqq a(1 + \| \log h \|)^d e^{-(1-\epsilon')\rho(\log h)}$$

for $m \in \omega$, $h \in A_I^+$ and $\lambda \in \mathfrak{F}_\epsilon$.

Now we come to the proof of Lemma 20. Since V is compact, we can choose a positive number a_2 such that $\beta(H) \geqq 2a_2$ for $H \in V$. Put $t_0 = \max(1, a_2^{-1})$ and select ϵ and ϵ' as in Lemma 21. We can assume that ϵ and ϵ' are so small that $\epsilon'\rho(H) \leqq a_2/2$ and $2r\,|\lambda_I(sH)| \leqq a_2/2$ for $H \in V$,

[10] For any $x \in G$, $| x |$ denotes the unique element $p \in \exp \mathfrak{p}_0$ such that $xp^{-1} \in K$. Moreover $\log | x | = X$ where $| x | = \exp X$ $(X \in \mathfrak{p}_0)$.

$s \in W$ and $\lambda \in \mathfrak{F}_\epsilon$. Therefore it follows from Lemma 18 and the corollary of Lemma 19 that we can select an integer $k_1 \geqq 0$ and a positive number a' such that

$$\| \Psi_H^0(\lambda : m ; \eta : tH) \| \leqq a'(1 + \| \lambda \|)^{k_1} t^r \exp\{t\rho(H) - 3ta_2/2\} \phi((-1)^{\frac{1}{2}}\lambda_I : m \exp tH)$$

if $m \in M_+$, $H \in V$, $t \geqq t_0$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand by Lemma 21,

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh \exp tH) \leqq a(1 + t \| H \|)^d e^{-(1-\epsilon')t\rho(H)} (1 + \| \log h \|)^d e^{-(1-\epsilon')\rho(\log h)}$$

for $m \in \omega$, $h \in A_1^+$ and $t \geqq t_0$. Moreover it is obvious that there exists a positive number c such that $\rho(H') \geqq c \| H' \|$ for $H' \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$. Therefore since $(1+t)^d e^{-(1-\epsilon')ct} \to 0$ as $t \to +\infty$, we can select a number $a'' > 0$ such that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh \exp tH) \leqq a'' t^d e^{-(1-\epsilon')t\rho(H)}$$

for $m \in \omega$, $h \in A_1^+$, $t \geqq t_0$ and $\lambda \in \mathfrak{F}_\epsilon$. This shows that

$$\| \Psi_H^0(\lambda : mh ; \eta : tH) \| \leqq a'a''(1 + \| \lambda \|)^{k_1} t^{r+d} \exp\{\epsilon' t\rho(H) - 3ta_2/2\}$$

under the same conditions. Therefore if we put $a_1 = a'a''$, $k = \max(k_1, r+d)$ and recall that $\epsilon'\rho(H) \leqq a_2/2$ for $H \in V$, the statement of Lemma 20 follows immediately.

7. The function Θ_H. Now fix an element H in $\mathfrak{l}_0^+$. Then if ϵ is sufficiently small, it follows from Lemma 20 and the corollary to Lemma 17 that for any $\eta \in \mathfrak{M}$, the integral

$$\int_0^\infty \| d\Phi^0(\lambda : m ; \eta : tH)/dt \| \, dt$$

converges uniformly as m and λ vary within compact subsets of M_+ and $\mathfrak{F}_\epsilon$ respectively. This shows that $\lim_{t \to +\infty} \Phi^0(\lambda : m : tH)$ exists and for a fixed m, it represents a holomorphic (matrix-) function of λ on $\mathfrak{F}_\epsilon$. We shall denote this limit by $\Theta_H(\lambda : m)$. Moreover in view of the uniform convergence of the above integral, the following facts are obvious. For a fixed λ in $\mathfrak{F}_\epsilon$, $\Theta_H(\lambda : m)$ is a C^∞ function of m on M_+ and $\Theta_H(\lambda : m ; \eta) = \lim_{t \to +\infty} \Phi^0(\lambda : m ; \eta : tH)$ for $\eta \in \mathfrak{M}$. Now suppose ω is a compact subset of M. Then we can obviously select a positive number t_0 such that $m \exp t_0 H \in M_+$ for $m \in \omega$. Also it follows from the definition of Φ^0 that

$$\Phi^0(\lambda : m : tH + t_0 H) = e^{t_0\rho(H)} \exp\{-t_0 \Xi(\lambda : H)\} \Phi^0(\lambda : m \exp t_0 H : tH).$$

Therefore if $\lambda \in \mathfrak{F}_\epsilon$ and $m \in \omega$,

$$\lim_{t \to +\infty} \Phi^0(\lambda : m : tH) = e^{t_0\rho(H)} \exp\{-t_0 \Xi(\lambda : H)\} \Theta_H(\lambda : m \exp t_0 H).$$

Hence we can extend Θ_H on $\mathfrak{F}_\epsilon \times M$ by setting

$$\Theta_H(\lambda : m) = \lim_{t \to +\infty} \Phi^0(\lambda : m : tH) \qquad (\lambda \in \mathfrak{F}_\epsilon, m \in M).$$

The following result is now obvious.

LEMMA 22. *$\Theta_H(\lambda : m \exp tH) = e^{-t\rho(H)} \exp(t\Xi(\lambda : H)) \Theta_H(\lambda : m)$ for $t \in R$, $m \in M$ and $\lambda \in \mathfrak{F}_\epsilon$.*

This lemma shows that for a fixed λ in $\mathfrak{F}_\epsilon$, Θ_H is a C^∞ function on M and for a fixed m in M, it is a holomorphic function on $\mathfrak{F}_\epsilon$.

LEMMA 23. *For any $\eta \in \mathfrak{M}$ we can select an integer k such that $(1 + \| \lambda \|)^{-k} \| \Theta_H(\lambda : m ; \eta) \|$ remains bounded for any fixed $m \in M$ as λ varies in $\mathfrak{F}_\epsilon$.*

Select $t_0 > 0$ such that $m_0 = m \exp t_0 H \in M_+$. Then

$$\Theta_H(\lambda : m ; \eta) = e^{t_0\rho(H)} \exp\{-t_0 \Xi(\lambda : H)\} \Theta_H(\lambda : m_0 ; \eta).$$

Hence in view of the corollary to Lemma 19, it is sufficient to consider the case when $m \in M_+$. But then

$$\Theta_H(\lambda : m ; \eta) = \Phi^0(\lambda : m ; \eta : TH) + \int_T^\infty \Psi_H{}^0(\lambda : m ; \eta : tH)\, dt$$

for $T \geqq 0$. Therefore

$$\| \Theta_H(\lambda : m ; \eta) \| \leqq \| \exp(-T\Xi(\lambda : H)) \| \, \| \Phi(\lambda : m ; \eta : TH) \| + \int_T^\infty \| \Psi_H{}^0(\lambda : m ; \eta : tH) \| \, dt.$$

On the other hand it follows from Lemma 46 of [2(i)] that

$$\| \Phi(\lambda : m ; \eta : TH) \| \leqq a_1 (1 + \| \lambda \|)^{k_1} \phi((-1)^{\frac{1}{2}} \lambda_I : m \exp TH) e^{T\rho(H)} \qquad (\lambda \in \mathfrak{F}_\epsilon, T \geqq 0)$$

where a_1 is a positive number and k_1 a nonnegative integer and the latter depends only on η. Hence if we apply Lemmas 20 and 21 and take into account the corollary of Lemma 19, our assertion becomes obvious.

Choose $\epsilon' > 0$ such that $\epsilon' \rho(H) < \beta(H)/3$ and $\epsilon' < 1$. We assume that ϵ is so small that the pair (ϵ, ϵ') fulfills the condition of Lemma 21 and $6r\epsilon \| H \| < \beta(H)$.

LEMMA 24. *Let q be an element in $I_{\mathfrak{g}}$. Then*

$$\Theta_H(\lambda : m ; \mu_0(q)) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda : m)$$

for $\lambda \in \mathfrak{F}_\epsilon$ and $m \in M$.

In view of Lemma 22, we may assume that $m \in M_+$. Now

$$\phi(\lambda : m ; \nu_i\mu_0(q)) = \phi(\lambda : m ; \nu_i q) - \phi(\lambda : m ; \nu_i \circ \mu(q)) \qquad (1 \leqq i \leqq r)$$

in the notation of Section 5. But $\phi(\lambda : m ; \nu_i q) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\phi(\lambda : m ; \nu_i)$ and $\nu_i\mu_0(q) - \mu_0(q)\nu_i \in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$ by Theorem 1 of [2(i)] since $\mu_0(q) \in I_{\mathfrak{m}}$. Therefore

$$\phi(\lambda : m ; \mu_0(q)\nu_i) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\phi(\lambda : m ; \nu_i) - \phi(\lambda : m ; \nu_i \circ \mu(q)).$$

Now fix m and λ. Then it follows from Lemmas 7 and 21 and [2(i), Lemma 46] that

$$|\phi(\lambda : m \exp tH ; \nu_i \circ \mu(q))| \leqq a(1+t)^d \exp\{-t\beta(H) - (1-\epsilon')t\rho(H)\} \qquad (t \geqq 0)$$

where a is a positive constant. Hence we can select a constant a_1 such that

$$\| \Phi(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi(\lambda : m : tH) \| \leqq a_1(1+t)^d e^{-2t\beta(H)/3} \qquad (t \geqq 0).$$

Therefore

$$\| \Phi^0(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi^0(\lambda : m : tH) \| \leqq a_1(1+t)^d e^{-2t\beta(H)/3} \| \exp(-t\Xi(\lambda : H)) \|.$$

In view of the inequality $6r\epsilon \| H \| \leqq \beta(H)$, it follows from the corollary of Lemma 19 that

$$\lim_{t \to +\infty} \| \Phi^0(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi^0(\lambda : m : tH) \| = 0.$$

This proves that $\Theta_H(\lambda : m ; \mu_0(q)) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda : m)$.

COROLLARY. *For a fixed λ in $\mathfrak{F}_\epsilon$, $\Theta_H(\lambda : m)$ is an analytic function of m on M.*

Let $Y_1, \cdots, Y_s$ be an orthonormal base for $\mathfrak{m}_{\mathfrak{l}_0}$ over R. Then it is easy to verify that $Y_1^2 + \cdots + Y_s^2 \in I_{\mathfrak{m}}$ and if ω is the Casimir operator of $\mathfrak{g}$, it follows from Lemma 14 that $\eta = \mu_0(\omega) + Y_1^2 + \cdots + Y_s^2$ is an elliptic differential operator (see Garding [1] for the definition of ellipticity) on M. On the other hand it is obvious from the definition of Θ_H that $\Theta_H(\lambda : k_1 m k_2)$

$=\Theta_H(\lambda:m)$ for $k_1, k_2 \in M_K$. Therefore $\Theta_H(\lambda:m;\eta)=\Theta_H(\lambda:m;\mu_0(\omega))$ $=\gamma(\omega:(-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda:m)$. This shows that for a fixed λ, every coefficient of the matrix Θ_H is an eigenfunction of η. Therefore since η is an analytic differential operator on M of the elliptic type, we can conclude (see John [3]) that all these coefficients are also analytic in m.

We shall now try to determine Θ_H explicitly.

LEMMA 25. *Let θ' be an analytic function on M such that $\theta'(k_1mk_2)=\theta'(m)$ for $k_1, k_2 \in M_K$ and $m \in M$ and suppose θ' is an eigenfunction of $\mu_0(q)$ for every $q \in I_\mathfrak{g}$. Then the equations $\theta'(1;\nu_i)=0$ $(1 \leqq i \leqq r)$ imply that θ' is identically zero.*

Let η be any element in $\mathfrak{M}$. Put $\eta_0=\int_{M_K}\eta^{k'}\,dk'$ where dk' denotes the normalized Haar measure on M_K. It is clear that $\theta'(1;\eta)=\theta'(1;\eta_0)$. But $\eta_0 \in I_\mathfrak{m}$ and $I_\mathfrak{m} \subset \sum_i \nu_i\mu_0(I_\mathfrak{g})+\mathfrak{M}\mathfrak{m}_\mathfrak{t}$ from Lemma 15. Hence it follows from our assumptions that $\theta'(1;\eta_0)=0$. This shows that $\theta'(1;\eta)=0$ for every $\eta \in \mathfrak{M}$. But since θ' is analytic, this means that $\theta'=0$.

For any $\lambda \in \mathfrak{F}$, put

$$\theta_\lambda(m)=\theta(\lambda:m)=\int_{M_K}\exp\{(-1)^{\frac{1}{2}}\lambda(H(mk'))-\rho(H(mk'))\}dk' \qquad (m \in M)$$

where dk' has the same meaning as above. Define $\gamma_\mathfrak{m}'(\eta)=e^{\rho-\sigma}\gamma_\mathfrak{m}(\eta)\circ e^{-\rho+\sigma}$ for $\eta \in I_\mathfrak{m}$ as in Section 5. Then by applying Lemma 18 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$), it follows without difficulty that

$$\theta(\lambda:m;\eta)=\gamma_\mathfrak{m}'(\eta:(-1)^{\frac{1}{2}}\lambda)\theta(\lambda:m) \qquad (\eta \in I_\mathfrak{g}),$$

where $\gamma_\mathfrak{m}'(\eta:(-1)^{\frac{1}{2}}\lambda)$ denotes the value of the polynomial function $\gamma_\mathfrak{m}'(\eta) \in S(\mathfrak{h}_\mathfrak{p})$ at $(-1)^{\frac{1}{2}}\lambda$. Therefore

$$\theta(\lambda:m;\mu_0(q))=\gamma(q:(-1)^{\frac{1}{2}}\lambda)\theta(\lambda:m) \qquad (q \in I_\mathfrak{g})$$

from Lemma 12.

Put $\nu_i=\gamma_\mathfrak{m}'(\nu_i)$ $1 \leqq i \leqq r$ and define π, π', $D=\pi/\pi'$ and τ^i $(1 \leqq i \leqq r)$ as in Lemma 15 of [2(i)]. Also put $\lambda^*=(-1)^{\frac{1}{2}}\lambda$ $(\lambda \in \mathfrak{F})$.

LEMMA 26. *Select r elements $s_1=1, s_2, \cdots, s_r$ in W such that $W=\bigcup_{1 \leqq i \leqq r} W's_i$. Then*

$$\pi(\lambda^*)\Theta_H(\lambda:m)=\sum_{1 \leqq i,j \leqq r}\epsilon(s_i)\pi'(s_i\lambda^*)\tau^j(s_i\lambda^*)\Theta_H(\lambda:1;\nu_j)\theta(s_i\lambda:m)$$

for $\lambda \in \mathfrak{F}_\epsilon$ and $m \in M$.

For a fixed m, both sides are holomorphic functions of λ. Hence it is enough to prove the above relation under the assumption that $\pi(\lambda) \neq 0$. Put $\lambda_i = s_i\lambda$. Then the rational functions $v^k = \tau^k/D$ on $\mathfrak{h}_\mathfrak{p}$ $(1 \leqq k \leqq r)$ are all defined at λ_i^* and we have to show that

$$f(\lambda : m) = \Theta_H(\lambda : m) - \sum_{1 \leqq i,j \leqq r} v^j(\lambda_i^*)\Theta_H(\lambda : 1 ; \nu_j)\theta(\lambda_i : m)$$

is zero. On the other hand $\theta(\lambda_i : m ; \nu_k) = v_k(\lambda_i^*)\theta(\lambda_i : m)$ and therefore

$$f(\lambda : 1 ; \nu_k) = \Theta_H(\lambda : 1 ; \nu_k) - \sum_{1 \leqq i,j \leqq r} v^j(\lambda_i^*)\Theta_H(\lambda : 1 ; \nu_j)v_k(\lambda_i^*).$$

But since $\mathrm{sp}_{J'/J}(v^j v_k) = \delta_k^j$ (see [2(i), § 3]), it follows that

$$\sum_i v^j(\lambda_i^*)v_k(\lambda_i^*) = \delta_k^j \qquad (1 \leqq j, k \leqq r)$$

and therefore $f(\lambda : 1 ; \nu_k) = 0$ $(1 \leqq k \leqq r)$. Hence our assertion is a consequence of Lemma 25.

8. The function Φ. We shall now show that if $\lambda \in \mathfrak{F}_R$, $\Theta_H(\lambda : m)$ is actually independent of H. Let H' be another element in $\mathfrak{l}_0^+$ and for a fixed $m \in M$, choose a positive number T_0' such that $m \exp T_0'H' \in M_+$. Then

$$\Phi^0(\lambda : m : TH + T'H') = \Phi^0(\lambda : m : T'H') + \int_0^T \{d\Phi^0(\lambda : m : tH + T'H')/dt\}dt$$

for $T, T' \geqq 0$. On the other hand

$$\Phi^0(\lambda : m : tH + T'H') = e^{T'\rho(H')} \exp(-T'\Xi(\lambda : H'))\Phi^0(\lambda : m \exp T'H' : tH)$$

from the definition of Φ^0. Therefore

$$\| d\Phi^0(\lambda : m : tH + T'H')/dt \| \leqq e^{T'\rho(H')} \| \exp(-T'\Xi(\lambda : H')) \| \, \| \Psi_H^0(\lambda : m \exp T'H' : tH) \|$$

for $t \geqq 0$ and $T' \geqq T_0'$. Now fix λ and m and assume that T_0' is sufficiently large. Then from Lemma 18 we can choose a constant a such that

$$\| d\Phi^0(\lambda : m : tH + T'H')/dt \| \leqq ae^{T'\rho(H')} \| \exp(-T'\Xi(\lambda : H')) \| \, \| \exp(-t\Xi(\lambda : H)) \| \times \exp\{t\rho(H) - t\beta(H) - T'\beta(H')\}\phi(0 : \exp(T'H' + tH))$$

for $T' \geqq T_0'$ and $t \geqq 0$. Hence in view of Theorem 3 of [2(i)] and the corollary of Lemma 19, we can find a positive number c and an integer $k \geqq 0$ such that

$$\| d\Phi^0(\lambda : m : tH + T'H')/dt \| \leqq c(1 + t)^k T'^k \exp\{-t\beta(H) - T'\beta(H')\} \qquad (T' \geqq T_0', t \geqq 0).$$

But this implies that

$$\lim_{T'\to+\infty}\int_0^\infty \| d\Phi^0(\lambda:m:tH+T'H')/dt\|\,dt=0$$

and therefore $\Phi^0(\lambda:m:TH+T'H')$ converges to $\lim_{t'\to+\infty}\Phi^0(\lambda:m:t'H')$ $=\Theta_{H'}(\lambda:m)$ as $T'\to+\infty$, uniformly with respect to T. Hence

$$\Theta_{H'}(\lambda:m)=\lim_{T,T'\to+\infty}\Phi^0(\lambda:m:TH+T'H').$$

But since the right side is symmetric with respect to H and H', we conclude that $\Theta_{H'}(\lambda:m)=\Theta_H(\lambda:m)$.

Now put $\Theta(\lambda:m)=\Theta_H(\lambda:m)$ $(\lambda\in\mathfrak{F}_R, m\in M)$ for any $H\in\mathfrak{l}_0^+$. We propose to obtain an estimate for the difference $\Phi^0-\Theta$.

LEMMA 27. *For any $\eta\in\mathfrak{M}$, we can choose an integer $k\geqq 0$ and a positive constant a such that*

$$\|\Phi^0(\lambda:h;\eta:H)-\Theta(\lambda:h;\eta)\|$$
$$\leqq a(1+\|\lambda\|)^k(1+\|H\|)^k e^{-\beta(H)}(1+\|\log h\|)^d e^{-\rho(\log h)}$$

for $\lambda\in\mathfrak{F}_R$, $h\in A_\mathfrak{p}^+$ and $H\in\mathfrak{l}_0^+$, provided $\beta(H)\geqq 1$. (Here d has the same meaning as in [2(i), Theorem 3].)

We know that

$$\Theta(\lambda:h;\eta)=\Phi^0(\lambda:h;\eta:H)+\int_1^\infty\{d\Phi^0(\lambda:h;\eta:tH)/dt\}dt.$$

Moreover

$$\|d\Phi^0(\lambda:h;\eta:tH)/dt\|=\|\Psi_H{}^0(\lambda:h;\eta:tH)\|$$
$$\leqq\|\exp(-t\Xi(\lambda:H))\|\,\|\Psi_H(\lambda:h;\eta:tH)\|.$$

Therefore it follows from Lemma 18 and the corollary to Lemma 19, that we can select integers $k_1,k_2\geqq 0$ and a positive number c_1 such that

$$\|d\Phi^0(\lambda:h;\eta:tH)/dt\|$$
$$\leqq c_1(1+\|\lambda\|)^{k_1}t^{k_2}(1+\|H\|)^{k_2}\exp\{t\rho(H)-t\beta(H)\}\phi(0:h\exp tH)$$

for $\lambda\in\mathfrak{F}_R$, $h\in A_\mathfrak{p}^+$, $H\in\mathfrak{l}_0^+$ and $t\geqq 1$ provided $\beta(H)\geqq 1$. On the other hand by Theorem 3 of [2(i)],

$$\phi(0:h\exp tH)\leqq c_2(1+\|\log h\|)^d(1+\|H\|)^d\exp\{-t\rho(H)-\rho(\log h)\}$$

where c_2 is a constant. Therefore

$$\|d\Phi^0(\lambda:h;\eta:tH)/dt\|\leqq c_1c_2(1+\|\lambda\|)^{k_1}t^{k_2}(1+\|H\|)^{k_2+d}$$
$$\times\exp\{-t\beta(H)-\rho(\log h)\}(1+\|\log h\|)^d.$$

But

$$\int_1^\infty t^{k_2} e^{-t\beta(H)} dt = e^{-\beta(H)} \int_0^\infty (1+t)^{k_2} e^{-t\beta(H)} dt$$

$$\leqq e^{-\beta(H)} \int_0^\infty (1+t)^{k_2} e^{-t}\, dt,$$

since $\beta(H) \geqq 1$. Therefore our assertion is now obvious.

COROLLARY. *For a given $\eta \in \mathfrak{M}$, we can chose an integer $k_1 \geqq 0$ and a positive number a_1 such that*

$$\| \Phi(\lambda : h ; \eta : H) - \exp \Xi(\lambda : H) \Theta(\lambda : h ; \eta) \|$$
$$\leqq a_1 (1 + \| \lambda \|)^{k_1} (1 + \| H \|)^{k_1} e^{-\beta(H)} (1 + \| \log h \|)^d e^{-\rho(\log h)}$$

for $\lambda \in \mathfrak{F}_R$, $h \in A_\mathfrak{p}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$.

This is an immediate consequence of the above lemma and the corollary to Lemma 19.

9. The functions $\boldsymbol{b}$ and $\boldsymbol{b}_0$. Define $\boldsymbol{b}$ as in Lemma 52 of [2(i)]. We intend to show that $|\boldsymbol{b}(s\lambda)| = |\boldsymbol{b}(\lambda)|$ for $s \in W$ and $\lambda \in \mathfrak{F}_R$. Let us say that $h \to \infty$ $(h \in A_\mathfrak{p}^+)$ if $\alpha(\log h) \to +\infty$ for every $\alpha \in P_+$. Moreover if f and g are two functions on $A_\mathfrak{p}^+$, we write $f(h) \sim g(h)$ if $\lim_{h \to \infty} |f(h) - g(h)| = 0$.

We now use the notation of Sections 7 and 8 and assume that ϵ is sufficiently small. Let $\mathfrak{F}_\epsilon'$ denote the set of those points $\lambda \in \mathfrak{F}_\epsilon$ where $\pi(\lambda) \neq 0$. Then it follows from Lemma 37 of [2(i)] (applied to $\mathfrak{m}$ instead of $\mathfrak{g}$) that there exists a holomorphic function $\boldsymbol{c}'$ on $\mathfrak{F}_\epsilon'$ such that[11]

$$e^{\rho(\log h)} \theta(\lambda : h) \sim \sum_{s \in W} \boldsymbol{c}'(s\lambda) \exp\{s\lambda^*(\log h)\} \qquad (h \in A_\mathfrak{p}^+)$$

for $\lambda \in \mathfrak{F}_\epsilon'$. Now let $\mathfrak{F}_R' = \mathfrak{F}_\epsilon' \cap \mathfrak{F}_R$ and fix $\lambda \in \mathfrak{F}_R'$ and $H \in \mathfrak{l}_0^+$. Put $\lambda_i = s_i\lambda$ and $f_i = f_{\lambda_i *}$ $(1 \leqq i \leqq r)$ in the notation of [2(i), Lemma 15]. Define the $r \times r$ matrix $F(i)$ with complex coefficients by

$$f_i v_j \equiv \sum_k F_{jk}(i)\, v_k \bmod S J_{\lambda *}.$$

Then if I is the unit matrix of degree r, it follows from Lemma 15 of [2(i)] that $\sum_i \epsilon(s_i) \pi'(\lambda_i^*) F(i) = \pi(\lambda^*) I$ and $F(i) \Xi(\lambda : h) = \lambda_i^*(H) F(i)$ $1 \leqq i \leqq r$. Hence

$$\pi(\lambda^*) \Phi^0(\lambda : h : tH) = \pi(\lambda^*) \exp(-t\Xi(\lambda : H)) \Phi(\lambda : h : tH)$$
$$= \sum_i \epsilon(s_i) \pi'(\lambda_i^*) e^{-t\lambda_i^*(H)} F(i) \Phi(\lambda : h : tH) \quad (t \in R, h \in A_\mathfrak{p}).$$

[11] If $s \in W$ and $\mu \in \mathfrak{F}$, $s\mu(H')$ denotes the value of the linear function $s\mu$ at $H' \in \mathfrak{h}_\mathfrak{p}$.

Therefore

$$\pi(\lambda^*)\Theta(\lambda:h) = \operatorname*{Lim}_{t\to+\infty} \sum_i \epsilon(s_i)\pi'(\lambda_i^*)e^{-t\lambda_i^*(H)}F(i)\Phi(\lambda:h:tH).$$

Now put $\phi'(\lambda:h) = e^{\rho(\log h)}\phi(\lambda:h)$. Since $v_i = \gamma_{\mathfrak{m}}'(v_i)$ $(1 \leqq i \leqq r)$, it follows without difficulty by applying Lemma 26 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$) that

$$\operatorname*{Lim}_{t\to+\infty} |\, \Phi_j(\lambda:h:tH) - \phi'(\lambda:h\exp tH\,;v_j)\,| = 0$$

for $h \in A_{\mathfrak{p}}^+$. Therefore

$$\pi(\lambda^*)e^{\rho(\log h)}\Theta_k(\lambda:h) = \operatorname*{Lim}_{t\to+\infty} \sum_{1\leqq i,j\leqq r} \epsilon(s_i)\pi'(\lambda_i^*)e^{-t\lambda_i^*(H)}F_{kj}(i)\phi'(\lambda:h\,\exp tH\,;v_j).$$

On the other hand it follows from Lemma 37 of [2(i)] that

$$\operatorname*{Lim}_{\substack{t\to+\infty \\ h\to\infty}} |\, \phi'(\lambda:h\exp tH\,;v_j) - \sum_{s\in W} \boldsymbol{c}(s\lambda)v_j(s\lambda^*)\exp\{s\lambda^*(\log h + tH)\}\,| = 0.$$

But we know from [2(i), Lemma 15] that $f_i v_k \equiv v_k(\lambda_i^*)f_i \bmod SJ_{\lambda^*}$ and therefore

$$\sum_j F_{kj}(i)v_j(\lambda_m^*) = v_k(\lambda_i^*)f_i(\lambda_m^*) = v_k(\lambda_i^*)\delta_{im}D(\lambda_i^*) \qquad (1 \leqq i,m \leqq r).$$

Moreover H is invariant under W', since it lies in the center of $\mathfrak{m}$. Hence

$$\begin{aligned}\sum_j F_{kj}(i) \sum_{s\in W} \boldsymbol{c}(s\lambda)v_j(s\lambda^*)e^{s\lambda^*(\log h+tH)} &= \sum_{j,m} F_{kj}(i)v_j(\lambda_m^*) \sum_{s'\in W'} \boldsymbol{c}(s'\lambda_m)e^{s'\lambda_m^*(\log h+tH)} \\ &= e^{t\lambda_i^*(H)}v_k(\lambda_i^*)D(\lambda_i^*) \sum_{s'\in W'} \boldsymbol{c}(s'\lambda_i)e^{s'\lambda_i^*(\log h)}.\end{aligned}$$

This proves that

$$\pi(\lambda^*)e^{\rho(\log h)}\Theta_k(\lambda:h) \sim \pi(\lambda^*) \sum_{1\leqq i\leqq r} v_k(\lambda_i^*) \sum_{s'\in W'} \boldsymbol{c}(s'\lambda_i)e^{s'\lambda_i^*(\log h)} \qquad (1 \leqq k \leqq r).$$

Now put (in the notation of Lemma 26)[12]

$$'\Gamma_{ki}(\lambda) = (-1)^{-d/2}\epsilon(s_i) \sum_{1\leqq j\leqq r} \tau^j(\lambda_i^*)\Theta_k(\lambda:1\,;v_j),$$

where d is the degree of $D = \pi/\pi'$. Then it follows from Lemma 26 that

$$\pi(\lambda)e^{\rho(\log h)}\Theta_k(\lambda:h) \sim \sum_{1\leqq i\leqq r} {}'\Gamma_{ki}(\lambda)\pi'(\lambda_i) \sum_{s'\in W'} \boldsymbol{c}'(s'\lambda_i)e^{s'\lambda_i^*(\log h)}.$$

This shows that

$$\operatorname*{Lim}_{h\to\infty} |\, \sum_i \sum_{s'\in W'} \{v_k(\lambda_i^*)\pi(\lambda)\boldsymbol{c}(s'\lambda_i) - {}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(s'\lambda_i)\}e^{s'\lambda_i^*(\log h)}\,| = 0.$$

---

[12] For any integer k, $(-1)^{k/2} = ((-1)^{\frac{1}{2}})^k$.

But since $\pi(\lambda) \neq 0$, the w elements $s'\lambda_i$ $(s' \in W', 1 \leqq i \leqq r)$ are all distinct. Hence we conclude from Lemma 57 of [2(i)] that

$$v_k(\lambda_i^*)\pi(\lambda)\boldsymbol{c}(s'\lambda_i) = {}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(s'\lambda_i) \qquad (s' \in W', 1 \leqq i, k \leqq r).$$

Putting $i = k = 1$ and ${}'\Gamma_{11} = \Gamma$, this becomes $\pi(\lambda)\boldsymbol{c}(s'\lambda) = \Gamma(\lambda)\pi'(\lambda)\boldsymbol{c}'(s'\lambda)$ $(\lambda \in \mathfrak{F}_R')$. Now if ϵ is sufficiently small, it follows from the results of Section 7, that ${}'\Gamma_{ij}$ can be extended to holomorphic functions on $\mathfrak{F}_\epsilon$. Moreover there exist (see [2(i), Lemma 52]) holomorphic functions $\boldsymbol{b}$ and $\boldsymbol{b}'$ on $\mathfrak{F}_\epsilon$ such that $\boldsymbol{b}(\lambda) = \pi(\lambda)\boldsymbol{c}(\lambda)$ and $\boldsymbol{b}'(\lambda) = \pi'(\lambda)\boldsymbol{c}'(\lambda)$ for $\lambda \in \mathfrak{F}_\epsilon'$. The above result shows that $\boldsymbol{b}(s'\lambda) = \Gamma(\lambda)\boldsymbol{b}'(s'\lambda)$ for $s' \in W'$ and $\lambda \in \mathfrak{F}_R'$. Hence by analytic continuation we obtain the following lemma.

LEMMA 28. *$\boldsymbol{b}(s'\lambda) = \Gamma(\lambda)\boldsymbol{b}'(s'\lambda)$ for $s' \in W'$ and $\lambda \in \mathfrak{F}_\epsilon$.*

COROLLARY 1. *$|\boldsymbol{b}(s\lambda)| = |\boldsymbol{b}(\lambda)|$ for $s \in W$ and $\lambda \in \mathfrak{F}_R$.*

It is obvious that $\phi(-\lambda : h) = \operatorname{conj}\phi(\lambda : h)$ for $\lambda \in \mathfrak{F}_R$ and $h \in A_\mathfrak{p}$. Hence it follows from Lemmas 37 and 57 of [2(i)] that $\boldsymbol{c}(-\lambda) = \operatorname{conj}\boldsymbol{c}(\lambda)$ for $\lambda \in \mathfrak{F}_R'$. Therefore if d is the degree of π, $\operatorname{conj}\boldsymbol{b}(\lambda) = (-1)^d\boldsymbol{b}(-\lambda)$ $(\lambda \in \mathfrak{F}_R)$. Let $l = \dim \mathfrak{h}_\mathfrak{p}$. If $l = 1$, W consists of only two elements. Hence if $s \neq 1$, $s\lambda = -\lambda$ and therefore our assertion is obvious. So now assume that $l \geqq 2$ and use induction. Define Σ as in [2(i), § 3]. Since the reflexions s_α $(\alpha \in \Sigma)$ generate W, it would be enough to prove that $|\boldsymbol{b}(s_\alpha\lambda)| = |\boldsymbol{b}(\lambda)|$ for $\alpha \in \Sigma$ and $\lambda \in \mathfrak{F}_R$. Now fix $\alpha \in \Sigma$ and select the element H_0 of Section 2 in such a way that $\alpha(H_0) = 0$. Then $s_\alpha \in W'$ and it follows by the induction hypothesis (applied to $\mathfrak{m}' = [\mathfrak{m}, \mathfrak{m}]$) that $|\boldsymbol{b}'(s'\lambda)| = |\boldsymbol{b}'(\lambda)|$ for $s' \in W'$ and $\lambda \in \mathfrak{F}_R$. But then by Lemma 27, $|\boldsymbol{b}(s_\alpha\lambda)| = |\Gamma(\lambda)\boldsymbol{b}'(s_\alpha\lambda)| = |\Gamma(\lambda)\boldsymbol{b}'(\lambda)|$ $= |\boldsymbol{b}(\lambda)|$. This proves our assertion.

COROLLARY 2. *$\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda) = \boldsymbol{b}(s\lambda)\boldsymbol{b}(-s\lambda)$ for $s \in W$ and $\lambda \in \mathfrak{F}_\epsilon$.*

First suppose $\lambda \in \mathfrak{F}_R$. Then we have seen above that

$$\boldsymbol{b}(-\lambda) = (-1)^d \operatorname{conj}\boldsymbol{b}(\lambda)$$

and therefore

$$\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda) = (-1)^d|\boldsymbol{b}(\lambda)|^2 = (-1)^d|\boldsymbol{b}(s\lambda)|^2 = \boldsymbol{b}(s\lambda)\boldsymbol{b}(-s\lambda)$$

by Corollary 1. Hence the same identity holds for all $\lambda \in \mathfrak{F}_\epsilon$ by analytic continuation.

COROLLARY 3. *Suppose ϵ is sufficiently small. Then if $\boldsymbol{b}(\lambda) = 0$ for some $\lambda \in \mathfrak{F}_\epsilon$, it follows that $\boldsymbol{b}(s\lambda) = 0$ for every $s \in W$.*

If $l=1$, our statement is true since $\boldsymbol{b}(\lambda)$ is never zero for $\lambda \in \mathfrak{F}_\epsilon$ (see Lemma 53 of [2(i)]). So let us assume that $l \geqq 2$ and use induction. Fix an element $\alpha \in \Sigma$. Obviously it would be enough to prove that $\boldsymbol{b}(s_\alpha \lambda)=0$. Again choose H_0 in such a way that $s_\alpha \in W'$. If $\boldsymbol{b}'(\lambda)=0$, it follows by induction hypothesis that $\boldsymbol{b}'(s_\alpha\lambda)=0$. On the other hand if $\boldsymbol{b}'(\lambda) \neq 0$, $\Gamma(\lambda)=\boldsymbol{b}(\lambda)/\boldsymbol{b}'(\lambda)=0$. Therefore in either case $\boldsymbol{b}(s_\alpha\lambda)=\Gamma(\lambda)\boldsymbol{b}'(s_\alpha\lambda)=0$.

Now we regard $\mathfrak{F}_\epsilon$ as a complex-analytic manifold and consider the divisor $\boldsymbol{d}$ of the function $\boldsymbol{b}$ on $\mathfrak{F}_\epsilon$. Select $\alpha_1, \cdots, \alpha_q \in \Sigma$ such that $\pi=\alpha_1\alpha_2\cdots\alpha_q$ and let $\boldsymbol{d}_i$ denote the divisor of α_i. Then it is obvious that $\boldsymbol{d}_i$ $(1 \leqq i \leqq q)$ are distinct prime divisors. Consider an element $\lambda \in \mathfrak{F}_\epsilon'$. We claim that $\boldsymbol{b}(\lambda) \neq 0$. For otherwise it follows from Corollary 3 of Lemma 28 that $\boldsymbol{b}(s\lambda)=0$ for every $s \in W$. But since $\pi(\lambda) \neq 0$, this implies that $\boldsymbol{c}(s\lambda)=0$ for all $s \in W$. However in view of [2(i), Lemma 37], this means that the analytic function ϕ_λ on $A_\mathfrak{p}$ must be identically zero. But this is impossible since $\phi(\lambda:1)=1$. Hence $\boldsymbol{b}(\lambda)$ is never zero unless $\pi(\lambda)=0$ $(\lambda \in \mathfrak{F}_\epsilon)$ and therefore $\boldsymbol{d}=k_1\boldsymbol{d}_1+\cdots+k_q\boldsymbol{d}_q$ where $k_1, \cdots, k_q$ are certain nonnegative integers. The divisors $\boldsymbol{d}_i$ are obviously invariant under the transformation $\lambda \to -\lambda$ of $\mathfrak{F}_\epsilon$. Hence $2\boldsymbol{d}$ is the divisor of the function $\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda)$. But then by Corollary 2 of Lemma 28, $\boldsymbol{d}$ must be invariant under W. We claim that $k_i \leqq 1$ $(1 \leqq i \leqq q)$. For otherwise suppose $k_1 \geqq 2$ and select a point $\lambda_0 \in \mathfrak{F}_R$ such that $\alpha_1(\lambda_0)=0$ while $\alpha_i(\lambda_0) \neq 0$ $(2 \leqq i \leqq q)$. Then $\boldsymbol{c}=\boldsymbol{b}/\pi$, considered as a meromorphic function on $\mathfrak{F}_\epsilon$, is holomorphic around λ_0 and $\boldsymbol{c}(\lambda_0)=0$. Since the divisor of $\boldsymbol{c}$ is invariant under W, it follows that $\boldsymbol{c}$ is holomorphic around $s\lambda_0$ and $\boldsymbol{c}(s\lambda_0)=0$ for every $s \in W$. Let U be a sufficiently small compact neighborhood of λ_0 in $\mathfrak{F}_R$. We now use the notation of [2(i), § 10]. Then if N is a sufficiently large positive number, $\Phi(s\lambda:h)$ is defined for $\lambda \in U$, $s \in W$ and $h \in A_\mathfrak{p}(N)$ and it follows from [2(i), Lemma 37] that

$$e^{\rho(\log h)}\phi(\lambda:h)=\sum_{s\in W}\boldsymbol{c}(s\lambda)\Phi(s\lambda:h) \qquad (h \in A_\mathfrak{p}(N))$$

for $\lambda \in U'=U \cap \mathfrak{F}_R'$. Hence if we fix $h \in A_\mathfrak{p}(N)$ and make λ tend to λ_0 it becomes clear (see [2(i), Corollary 2 of Lemma 28]) that

$$e^{\rho(\log h)}\phi(\lambda_0:h)=\sum_{s\in W}\boldsymbol{c}(s\lambda_0)\Phi(s\lambda_0:h)=0 \qquad (h \in A_\mathfrak{p}(N)).$$

However this is impossible because the analytic function ϕ_{λ_0} on $A_\mathfrak{p}$ is not identically zero. In fact $\phi(\lambda_0:1)=1$. This proves that $k_i=0$ or 1 $(1 \leqq i \leqq q)$. Hence we may assume that the divisor of $\boldsymbol{c}^{-1}$ is $\boldsymbol{d}_1+\boldsymbol{d}_2+\cdots+\boldsymbol{d}_p$ for some integer p $(0 \leqq p \leqq q)$. Put $\pi_0=\alpha_1\alpha_2\cdots\alpha_p$. $(\pi_0=1$ if $p=0.)$ Since

$\boldsymbol{d}_1 + \cdots + \boldsymbol{d}_p$ is invariant under W, it is clear that $\pi_0{}^s = \epsilon_0(s)\pi_0$ $(s \in W)$ where $\epsilon_0(s) = \pm 1$. Put $\boldsymbol{b}_0 = \pi_0 \boldsymbol{c}$. Then the divisor of $\boldsymbol{b}_0$ is zero. Hence we have obtained the following result.

LEMMA 29. *The functions $\boldsymbol{c}^{-1}$ and $\boldsymbol{b}_0 = \pi_0 \boldsymbol{c}$ are everywhere holomorphic on $\mathfrak{F}_\epsilon$. Moreover $\boldsymbol{b}_0$ is nowhere zero on $\mathfrak{F}_\epsilon$.*

Define $\boldsymbol{b}_0'$ and π_0' in an analogous way (corresponding to $\mathfrak{m}$). Then $\boldsymbol{b}_0' = \pi_0' \boldsymbol{c}'$ and $\boldsymbol{b}_0'$, $1/\boldsymbol{b}_0'$ are both holomorphic on $\mathfrak{F}_\epsilon$. Put $\pi_1 = \pi/\pi_0$, $\pi_1' = \pi'/\pi_0'$. Then $\boldsymbol{b}_0 = \Gamma\pi_1' \boldsymbol{b}_0'/\pi_1$. But since $\boldsymbol{b}_0$ and $\boldsymbol{b}_0'$ have no zeros, it follows that $\Gamma_0 = \Gamma\pi_1'/\pi_1$ and its reciprocal are both holomorphic on $\mathfrak{F}_\epsilon$. Moreover we saw during the proof of Lemma 28 that

$$v_k(\lambda_i{}^*)\pi(\lambda)\boldsymbol{c}(\lambda_i) = {}^t\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(\lambda_i) \qquad (1 \leqq i, k \leqq r)$$

for $\lambda \in \mathfrak{F}_R'$. But $\pi(\lambda)\boldsymbol{c}(\lambda_i) = \epsilon(s_i)\boldsymbol{b}(\lambda_i) = \epsilon(s_i)\Gamma(\lambda_i)\boldsymbol{b}'(\lambda_i)$. Also $\boldsymbol{b}'(\lambda_i) \neq 0$ since $\pi(\lambda) \neq 0$ (Corollary 3 of Lemma 28). Therefore

$${}^t\Gamma_{ki}(\lambda) = \epsilon(s_i)v_k(s_i\lambda^*)\Gamma(s_i\lambda) \qquad (1 \leqq i, k \leqq r)$$

and so, by analytic continuation, this relation holds for all $\lambda \in \mathfrak{F}_\epsilon$. Put $\Gamma_{ki}(\lambda) = \epsilon_0(s_i)v_k(s_i\lambda^*)\Gamma_0(s_i\lambda)$ $(1 \leqq i, k \leqq r, \lambda \in \mathfrak{F}_\epsilon)$. Then it follows from Lemma 26 and the definition of ${}^t\Gamma_{ki}(\lambda)$ that

$$\pi_0(\lambda)\Theta_k(\lambda : m) = \sum_{1 \leqq i \leqq r} \Gamma_{ki}(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i : m) \qquad (m \in M)$$

for $\lambda \in \mathfrak{F}_R'$. Therefore since both sides are analytic functions of λ, this holds for all $\lambda \in \mathfrak{F}_R$.

LEMMA 30. *There exist analytic functions Γ_{ij} $1 \leqq i, j \leqq r$ on $\mathfrak{F}_R$ with the following properties.*

(1) $$\pi_0(\lambda)\Theta_i(\lambda : m) = \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda)\pi_0'(s_j\lambda)\theta(s_j\lambda : m)$$
$$(1 \leqq i \leqq r, \lambda \in \mathfrak{F}_R, m \in M).$$

(2) *We can find an integer $d \geqq 0$ such that*

$$(1 + \| \lambda \|)^{-d} \sum_{i,j} | \Gamma_{ij}(\lambda; \partial(v)) |$$

remains bounded for any fixed $v \in S(\mathfrak{h}_\mathfrak{p})$ as λ varies in $\mathfrak{F}_R$.

In order to verify the second property we proceed as follows. In view of Lemma 58 of [2(i)] and the definition of Γ_{ij}, it would be enough to show that $\sup_{\lambda \in \mathfrak{F}_{\epsilon'}} (1 + \| \lambda \|)^{-d} | \Gamma_0(\lambda) | < \infty$ for some $\epsilon' > 0$ and $d \geqq 0$. Since $\Gamma_0 = \Gamma\pi_1'/\pi_1$ and Γ_0 has no zeros on $\mathfrak{F}_\epsilon$, it follows that π_1' divides π_1 in

$S(\mathfrak{h}_\mathfrak{p})$. Therefore by the corollary of Lemma 59 of [2(i)], it would be sufficient to verify that $\sup_{\lambda \in \mathfrak{F}_\epsilon} (1 + \| \lambda \|)^{-d} |\Gamma(\lambda)| < \infty$ for some $d \geqq 0$. But $\Gamma(\lambda) = {}^t\Gamma_{11}(\lambda)$ and so this follows immediately from Lemma 23 and the definition of ${}^t\Gamma_{11}$.

If we take into account Lemma 52 of [2(i)], we get the following result by a similar argument.

LEMMA 31. *We can select an integer $d \geqq 0$ with the following property. For any $u \in S(\mathfrak{h}_\mathfrak{p})$, $\sup_{\lambda \in \mathfrak{F}_R} (1 + \| \lambda \|)^{-d} |\boldsymbol{b}_0(\lambda; \partial(u))|$ is finite.*

The following lemma will be needed in Section 13.

LEMMA 32. *Let p be an element in $S(\mathfrak{h}_\mathfrak{p})$ such that $p^s = \epsilon_0(s)p$ $(s \in W)$. Then $p = \pi_0 q$ for some $q \in I(\mathfrak{h}_\mathfrak{p})$.*

Fix an element $\alpha \in \Sigma$. It follows easily (see the proof of Lemma 10 of [2(i)]) that $\epsilon_0(s_\alpha) = -1$ or 1 according as α divides π_0 or not. Now suppose α divides π_0. Then $p^{s_\alpha} = -p$ and therefore α divides p. This shows that π_0 divides p in $S(\mathfrak{h}_\mathfrak{p})$ and our assertion is now obvious.

10. The relationship between φ and θ. Lemmas 27 and 30 give us an approximate connection between the functions ϕ and θ. Since I lies in the center of $\mathfrak{m}$, it is obvious that $\theta(\lambda : m \exp H) = \exp\{\lambda^*(H) - \rho(H)\}\theta(\lambda : m)$ for $H \in \mathfrak{l}_0$, $\lambda \in \mathfrak{F}$ and $m \in M$. Therefore it follows from Lemma 30 that

$$\pi_0(\lambda) e^{\rho(H)} \Theta_i(\lambda : m \exp(H)) = \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : m) \qquad (1 \leqq i \leqq r).$$

On the other hand

$$\Phi_i(\lambda : h ; \eta : H) = e^{\rho(H)} \phi(\lambda : h \exp H ; \eta \nu_i) \qquad (1 \leqq i \leqq r)$$

for $\eta \in \mathfrak{M}$. Therefore we get the following result from the corollary of Lemma 27.

LEMMA 33. *For a given $\eta \in \mathfrak{M}$, we can choose an integer $k \geqq 0$ and a positive number a such that*

$$|\pi_0(\lambda) e^{\rho(\log h + H)} \phi(\lambda : h \exp H ; \eta \nu_i) - \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : h ; \eta) e^{\rho(\log h)}|$$

$$\leqq a(1 + \| \lambda \|)^k (1 + \| H \|)^k e^{-\beta(H)} (1 + \| \log h \|)^d \qquad (1 \leqq i \leqq r)$$

for $\lambda \in \mathfrak{F}_R$, $h \in A_\mathfrak{p}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$. (Here d has the same meaning as in [2(i), Theorem 3].)

Now fix an element $b \in \mathfrak{B}$ and consider the differential operators $\mu_0(b)$ and $\mu(b)$ of Lemma 10. Then $\mu(b) = \sum_{1 \leqq i \leqq s} g_i \eta_i$ where $g_i \in \mathfrak{R}_0$ and $\eta_i \in \mathfrak{M}_\mathfrak{p}$. From Lemma 7, we can select a positive number a_1 such that $|g_i(h \exp H)| \leqq a_1 e^{-\beta(H)}$ for $h \in A_\mathfrak{p}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$. Hence

$$|\phi(\lambda : h \exp H ; \mu(b))| \leqq a_1 e^{-\beta(H)} \sum_{1 \leqq j \leqq s} |\phi(\lambda : h \exp H ; \eta_j)|.$$

On the other hand by Lemma 46 of [2(i)], there exists an integer $k_1 \geqq 0$ and a constant $a_2 > 0$ such that

$$\sum_{1 \leqq j \leqq s} |\phi(\lambda : h \exp H ; \eta_j)| \leqq a_2(1 + \|\lambda\|)^{k_1}(1 + \|H\|)^d(1 + \|\log h\|)^d e^{-\rho(H + \log h)}$$

for all $\lambda \in \mathfrak{F}_R$. This shows that

$$\begin{aligned} &e^{\rho(H+\log h)} |\phi(\lambda : h \exp H ; b) - \phi(\lambda : h \exp H ; \mu_0(b))| \\ &= e^{\rho(H+\log h)} |\phi(\lambda : h \exp H ; \mu(b))| \\ &\leqq a_1 a_2 (1 + \|\lambda\|)^{k_1} e^{-\beta(H)} (1 + \|H\|)^d (1 + \|\log h\|)^d \quad (h \in A_\mathfrak{p}^+, H \in \mathfrak{l}_0^+) \end{aligned}$$

provided $\beta(H) \geqq 1$. Since $\mu_0(b) \in \mathfrak{M}$ and $\nu_1 = 1$, we can now apply Lemma 33 to $\eta = \mu_0(b)$ and thus obtain the following result. Put $\Gamma_j(\lambda) = \Gamma_{1j}(\lambda)$ $(1 \leqq j \leqq r)$.

LEMMA 34. *For any $b \in \mathfrak{B}$, we can choose an integer $k \geqq 0$ and a positive number a such that*

$$\begin{aligned} &|\pi_0(\lambda) e^{\rho(\log h + H)} \phi(\lambda : h \exp H ; b) \\ &\qquad - \sum_{1 \leqq j \leqq r} \Gamma_j(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : h ; \mu_0(b)) e^{\rho(\log h)}| \\ &\qquad\qquad \leqq a(1 + \|\lambda\|)^k (1 + \|H\|)^k e^{-\beta(H)} (1 + \|\log h\|)^d \end{aligned}$$

for $\lambda \in \mathfrak{F}_R$, $h \in A_\mathfrak{p}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$.

We recall that the element H_0 of Section 2 has been kept fixed throughout our discussion. It is obvious that $\rho(H_0) > 0$. Select a number ϵ such that $0 < \epsilon < 1$ and let U be the set of all points $H \in \mathfrak{h}_{\mathfrak{p}_0}$ which satisfy the conditions $\alpha(H) \geqq (1 - \epsilon)\alpha(H_0)$ $(\alpha \in P)$ and $\|H\| \leqq (1 + \epsilon)\|H_0\|$. Then U is a neighborhood of H_0 in $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$. Put $H_\epsilon = H - (1 - \epsilon)H_0$ for $H \in U$. Then $H_\epsilon \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ and $\exp tH = \exp t(1 - \epsilon)H_0 \exp tH_\epsilon$ $(t \in R)$. Hence if $t \geqq t_0 = \{(1 - \epsilon)\beta(H_0)\}^{-1}$, it follows from Lemma 34 that

$$\begin{aligned} &|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b) \\ &\qquad - \sum_{1 \leqq i \leqq r} \Gamma_i(\lambda) \exp\{t(1 - \epsilon)\lambda_i^*(H_0)\} \pi_0'(\lambda_i) \theta(\lambda_i : \exp tH_\epsilon ; \mu_0(b)) e^{t\rho(H_\epsilon)}| \\ &\qquad\qquad \leqq a(1 + \|\lambda\|)^k (1 + \|tH_0\|)^k (1 + \|tH_\epsilon\|)^d e^{-t/t_0} \end{aligned}$$

for $H \in U$ and $\lambda \in \mathfrak{F}_R$. Moreover since H_0 lies in the center of $\mathfrak{m}$, it is clear that

$$\theta(\lambda_i : \exp tH ; \mu_0(b)) = \exp\{t(1-\epsilon)\lambda_i^*(H_0) - t(1-\epsilon)\rho(H)\}\theta(\lambda_i : \exp tH_\epsilon ; \mu_0(b)).$$

Also $\| H_\epsilon \| \leqq \| H \| + (1-\epsilon)\| H_0 \| \leqq 2 \| H_0 \|$. Therefore if we put $a_1 = 2^d(1 + \| H_0 \|)^{k+d}a$, it follows that

$$|\pi_0(\lambda)e^{t\rho(H)}\phi(\lambda : \exp tH ; b) - \sum_i \Gamma_i(\lambda)\pi_0'(\lambda_i)e^{t\rho(H)}\theta(\lambda_i : \exp tH ; \mu_0(b))|$$
$$\leqq a_1(1 + \| \lambda \|)^k(1+t)^{k+d}e^{-t/t_0}$$

for $H \in U$, $\lambda \in \mathfrak{F}_R$ and $t \geqq t_0$. On the other hand by applying Lemma 46 and Theorem 3 of [2(i)] both to $\phi(\lambda : \exp tH ; b)$ and $\theta(\lambda_i : \exp tH ; \mu_0(b))$ and making use of the second statement of Lemma 30, we conclude that

$$|\pi_0(\lambda)\phi(\lambda : h ; b)| + \sum_i |\Gamma_i(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i : h ; \mu_0(b))|$$
$$\leqq a_2(1 + \| \lambda \|)^{k_2}e^{-\rho(\log h)}(1 + \| \log h \|)^{d_2}$$

for suitable constants $a_2, k_2, d_2 \geqq 0$ and $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$, $\lambda \in \mathfrak{F}_R$. Since $\lim_{t \to +\infty} t^q e^{-t/2t_0} = 0$ for any $q \geqq 0$, we thus obtain the following result.

LEMMA 35. *There exists a neighborhood U of H_0 in $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ and a positive number t_0 with the following property. If b is any given element in $\mathfrak{B}$, we can select an integer $k \geqq 0$ and a constant $a > 0$ such that*

$$|\pi_0(\lambda)e^{t\rho(H)}\phi(\lambda : \exp tH ; b) - \sum_i \Gamma_i(\lambda)\pi_0'(\lambda_i)e^{t\rho(H)}\theta(\lambda_i : \exp tH ; \mu_0(b))|$$
$$\leqq a(1 + \| \lambda \|)^k e^{-t/2t_0}$$

for $H \in U$, $\lambda \in \mathfrak{F}_R$ and $t \geqq 0$.

11. Proof of Theorem 1. We shall now deduce an important result from Lemma 35.

THEOREM 1. *For any $b \in \mathfrak{B}$, we can choose an integer $k \geqq 0$ such that $(1 + \| \lambda \|)^{-k}|\pi_0(\lambda)\phi(\lambda : h ; b)e^{\rho(\log h)}|$ remains bounded as λ and h vary in $\mathfrak{F}_R$ and $\mathrm{Cl}(A_\mathfrak{p}^+)$ respectively.*

We shall prove this theorem by induction on $\dim_R \mathfrak{g}_0$. Let S_+ be the set of all points $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ with $\| H \| = 1$. Then S_+ is compact. Therefore it is obviously sufficient to prove the following lemma.

LEMMA 36. *For a given $b \in \mathfrak{B}$ and $H_0 \in S_+$, we can choose a neighborhood V of H_0 in S_+, an integer $k_1 \geqq 0$ and a positive number a_1 such that*

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b)| \leqq a_1(1 + \|\lambda\|)^{k_1}$$

for $\lambda \in \mathfrak{F}_R$, $H \in V$ and $t \geqq 0$.

We now construct $\mathfrak{m}_0$ corresponding to this H_0 and use the notation of Lemma 35. Since $\mathfrak{m}_0$ is reductive, its derived algebra $\mathfrak{m}_0' = [\mathfrak{m}_0, \mathfrak{m}_0]$ is semi-simple and $\dim_R \mathfrak{m}_0' < \dim_R \mathfrak{g}_0$ because H_0 lies in the center of $\mathfrak{m}_0$. Therefore our induction hypothesis is applicable to $\mathfrak{m}_0'$. Define σ as in Lemma 12 and put

$$\theta'(\lambda : m) = \int_{M_K} \exp\{\lambda^*(H(mk')) - \sigma(H(mk'))\} dk' \qquad (\lambda \in \mathfrak{F}_R, m \in M),$$

where dk' denotes, as before, the normalized Haar measure of M_K. Now $\mathfrak{l}_0$ lies in the center of $\mathfrak{m}_0$ and $\mathfrak{m}_0 = \mathfrak{l}_0 + \mathfrak{m}_0' + \mathfrak{m}_{\mathfrak{k}_0}$. Hence by applying the induction hypothesis to $\mathfrak{m}_0'$, it is easily seen that for any $\eta \in \mathfrak{M}$, we can select an integer $k_2 \geqq 0$ and a positive number a_2 such that

$$|\pi_0'(\lambda) e^{\sigma(H)} \theta'(\lambda : \exp H ; \eta)| \leqq a_2(1 + \|\lambda\|)^{k_2}$$

for all $\lambda \in \mathfrak{F}_R$ and $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$. Also it is obvious that

$$\theta(\lambda : h) = \exp(\sigma(\log h) - \rho(\log h)) \theta'(\lambda : h)$$

for $h \in A_{\mathfrak{p}}$. Let $\mu_0(b)'$ denote the image of $\mu_0(b)$ under the automorphism of $\mathfrak{M}$ over C which leaves every element of $\mathfrak{m}_0' + \mathfrak{m}_{\mathfrak{k}_0}$ fixed and maps H on $H - \rho(H)$ for $H \in \mathfrak{l}$. Then clearly

$$\theta(\lambda : h ; \mu_0(b)) = \exp(\sigma(\log h) - \rho(\log h)) \theta'(\lambda : h ; \mu_0(b)')$$

and therefore if we take $\eta = \mu_0(b)'$, it follows that

$$|\pi_0'(\lambda) e^{\rho(H)} \theta(\lambda : \exp H ; \mu_0(b))| \leqq a_2(1 + \|\lambda\|)^{k_2}$$

for $\lambda \in \mathfrak{F}_R$ and $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$. But then from the second statement of Lemma 30, we can conclude that

$$|\sum_i \pi_0'(\lambda_i) \Gamma_i(\lambda) e^{\rho(H)} \theta(\lambda_i : \exp H ; \mu_0(b))| \leqq a_3(1 + \|\lambda\|)^{k_3} \qquad (\lambda \in \mathfrak{F}_R, H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+))$$

for suitable constants $a_3, k_3 \geqq 0$. Hence it follows from Lemma 35 that we can choose constants $a_1, k_1 \geqq 0$ and a neighborhood V of H_0 in S_+ such that

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b)| \leqq a_1(1 + \|\lambda\|)^{k_1}$$

for $H \in V$, $\lambda \in \mathfrak{F}_R$ and $t \geqq 0$. This proves Lemma 36 and hence also Theorem 1.

12. The space $I(G)$. Let x be an element in G. Then x can be written uniquely (see [2(f), Lemma 31]) in the form $k \exp X$ $(k \in K, X \in \mathfrak{p}_0)$. Put $D(x) = \{\det(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{p}}\}^{\frac{1}{2}}$, where $(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{p}}$ denotes the restriction on $\mathfrak{p}$ of the linear transformation

$$\sinh \operatorname{ad} X/\operatorname{ad} X = \sum_{q \geqq 0} (\operatorname{ad} X)^{2q}/(2q+1)!$$

of $\mathfrak{g}$. Then D is an analytic function on G which is obviously spherical. Put[10] $D_q(x) = (1 + \| \log |x| \|)^q D(x)$.

DEFINITION. *Let $I(G)$ denote the set of all complex-valued functions ϕ on G of class C^∞ satisfying the following two conditions:*

(1) *ϕ is spherical.*

(2) *For any $b \in \mathfrak{B}$ and any integer $q \geqq 0$,*

$$\sup_{x \in G} D_q(x) |\phi(x; b)| < \infty.$$

Put $\tau_{b,q}(\phi) = \sup D_q(x) |\phi(x; b)|$. Then $\tau_{b,q}$ is a seminorm on $I(G)$ and the collection of these seminorms, for all $b \in \mathfrak{B}$ and $q \geqq 0$, defines a topology on $I(G)$ in the usual way so that $I(G)$ becomes a locally convex space.

We note that $(e^t - e^{-t})/2t = \sum_{q \geqq 0} t^{2q}/(2q+1)!$ is an increasing function of t for $t \geqq 0$. Hence it follows easily that $D(x) \geqq D(1) = 1$ $(x \in G)$. Moreover $(1 - e^{-2t})/2t$ remains bounded for $t \geqq 0$ and therefore $D(h) e^{-\rho(\log h)}$ also remains bounded as h varies in $\mathrm{Cl}(A_{\mathfrak{p}}^+)$. We shall need these facts presently.

THEOREM 2. *For any $b \in \mathfrak{B}$, we can select an integer $q \geqq 0$ and a constant $c > 0$ such that*

$$D(x) |\pi_0(\lambda) \phi(\lambda : x; b)| \leqq c(1 + \| \lambda \|)^q$$

for all $x \in G$ and $\lambda \in \mathfrak{F}_R$.

Obviously we can choose a finite number of elements $b_1, \cdots, b_r \in \mathfrak{B}$ and analytic functions $a_1, \cdots, a_r$ on K such that $b^k = \sum_{1 \leqq i \leqq r} a_i(k) b_i$ for $k \in K$. Now suppose $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$ and $k \in K$. Then

$$\phi(\lambda : hk; b) = \phi(\lambda : h; b^k) = \sum_i a_i(k) \phi(\lambda : h; b_i)$$

and therefore

$$|\phi(\lambda : hk; b)| \leqq a \sum_i |\phi(\lambda : h; b_i)|$$

where $a = \sup_{k \in K} (|a_1(k)|, \cdots, |a_r(k)|)$. On the other hand $D(hk) = D(h)$

and $D(h)e^{-\rho(\log h)}$ remains bounded as h varies in $\mathrm{Cl}(A_{\mathfrak{p}}^+)$. Therefore by Theorem 1, we can choose an integer $q \geqq 0$ and a constant $c > 0$ such that

$$D(h)\,|\,\pi_0(\lambda)\phi(\lambda : hk; b)\,| \leqq c(1 + \|\lambda\|)^q$$

for all $\lambda \in \mathfrak{F}_R$, $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$ and $k \in K$. But $G = K(\mathrm{Cl}(A_{\mathfrak{p}}^+))K$ (see [2(f), § 12]) and D and ϕ_λ are spherical functions. Hence it is clear that

$$D(x)\,|\,\pi_0(\lambda)\phi(\lambda : x; b)\,| \leqq c(1 + \|\lambda\|)^q$$

for $x \in G$ and $\lambda \in \mathfrak{F}_R$. This proves the theorem.

Now $\mathfrak{F}_R$ being a real Euclidean space, we can define the locally convex space $\mathcal{B}(\mathfrak{F}_R)$ as usual (see [2(g), § 2]). It consists of all complex-valued C^∞ functions a on $\mathfrak{F}_R$ such that $\sup_{\lambda \in \mathfrak{F}_R} (1 + \|\lambda\|)^q\,|\,a(\lambda; \partial(p)\,| < \infty$ for $p \in S(\mathfrak{h}_{\mathfrak{p}})$ and any integer $q \geqq 0$. Let $d\lambda$ denote the Euclidean measure on $\mathfrak{F}_R$. Then if $a \in \mathcal{B}(\mathfrak{F}_R)$, it follows from Theorem 2 that the integral

$$\int_{\mathfrak{F}_R} |\,\pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\,|\,d\lambda \qquad (b \in \mathfrak{B})$$

converges uniformly with respect to $x \in G$. This shows that

$$\phi_a(x) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x)\,d\lambda \qquad (x \in G)$$

is a C^∞ function on G and

$$\phi_a(x; b) = \int \pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\,d\lambda \qquad (b \in \mathfrak{B}).$$

THEOREM 3. *For any $a \in \mathcal{B}(\mathfrak{F}_R)$, put*

$$\phi_a(x) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x)\,d\lambda \qquad (x \in G).$$

Then $\phi_a \in I(G)$ and $a \to \phi_a$ is a continuous mapping of $\mathcal{B}(\mathfrak{F}_R)$ into $I(G)$. Also

$$\phi_a(x; b) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\,d\lambda \qquad (x \in G, b \in \mathfrak{B}).$$

It is obvious from its definition that ϕ_a is spherical. Moreover if $x = k_1hk_2$ $(k_1, k_2 \in K; h \in \mathrm{Cl}(A_{\mathfrak{p}}^+))$, it is clear that

$$D_r(x)\phi_a(x; b) = D_r(h)\phi_a(h; b^{k_2})$$

for $b \in \mathfrak{B}$ and any integer $r \geqq 0$. Let $\mathfrak{D}(\mathfrak{h}_{\mathfrak{p}})$ denote the algebra of polynomial differential operators on $\mathfrak{h}_{\mathfrak{p}}$ (see [2(g), § 2]). Then as we saw during the proof of Theorem 2, it would be sufficient to prove the following lemma.

LEMMA 37. *Let b be an element in $\mathfrak{B}$ and s an integer $\geqq 0$. Then we can select a finite number of elements $d_0, d_1, \cdots, d_N$ in $\mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that*

$$(1+\|\log h\|)^s e^{\rho(\log h)}\,|\,\phi_a(h;b)\,| \leqq \sum_{0\leqq i\leqq N} \sup_{\lambda\in\mathfrak{F}_R} |\,a(\lambda;d_i)\,|$$

for $a\in\mathcal{B}(\mathfrak{F}_R)$ and $h\in \mathrm{Cl}(A_\mathfrak{p}^+)$.

We shall use induction on $\dim \mathfrak{h}_\mathfrak{p}$. The case $\mathfrak{h}_\mathfrak{p}=\{0\}$ is obviously trivial. So let us assume that $\dim \mathfrak{h}_\mathfrak{p}\geqq 1$. Define S_+ as in Section 11. Since S_+ is compact, it would be enough to prove the following statement.

LEMMA 38. *Fix b and s as above. Then for a given $H_0\in S_+$, we can select a neighborhood V of H_0 in S_+ and a finite number of elements $d_0,\cdots,d_N\in\mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that*

$$(1+t)^s e^{t\rho(H)}\,|\,\phi_a(\exp tH;b)\,| \leqq \sum_{0\leqq i\leqq N} \sup_{\lambda\in\mathfrak{F}_R} |\,a(\lambda;d_i)\,|$$

for $a\in\mathcal{B}(\mathfrak{F}_R)$, $H\in V$ and $t\geqq 0$.

We use the notation of Lemma 35 (corresponding to the element H_0 selected above). Then by this lemma, we can choose a neighborhood V of H_0 in S_+, an integer $k\geqq 0$ and two constants c, $t_0>0$ such that

$$|\,\pi_0(\lambda)e^{t\rho(H)}\phi(\lambda:\exp tH;b) - \sum_{1\leqq i\leqq r}\Gamma_i(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i:\exp tH;\mu_0(b))e^{t\rho(H)}\,|$$
$$\leqq c(1+\|\lambda\|)^k e^{-t/t_0}$$

for $H\in V$, $\lambda\in\mathfrak{F}_R$ and $t\geqq 0$. Put

$$f_a(m)=\int_{\mathfrak{F}_R}\pi_0'(\lambda)a(\lambda)\theta(\lambda:m)\,d\lambda \qquad (m\in M, a\in\mathcal{B}(\mathfrak{F}_R)).$$

Then by induction hypothesis, Lemma 37 is applicable to $\mathfrak{m}_0'=[\mathfrak{m}_0,\mathfrak{m}_0]$ instead of $\mathfrak{g}_0$ and so it follows easily that we can choose a finite number of elements $d_1',\cdots,d_p'\in\mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that

$$(1+\|\log h\|)^s e^{\rho(\log h)}\,|\,f_a(h;\mu_0(b))\,| \leqq \sum_{1\leqq i\leqq p}\sup_{\lambda\in\mathfrak{F}_R}|\,a(\lambda;d_i')\,|$$

for $a\in\mathcal{B}(\mathfrak{F}_R)$ and $h\in\mathrm{Cl}(A_\mathfrak{p}^+)$. Now put $a_i(\lambda)=\Gamma_i(s_i^{-1}\lambda)a(s_i^{-1}\lambda)$ $(1\leqq i\leqq r)$ for $a\in\mathcal{B}(\mathfrak{F}_R)$ and $\lambda\in\mathfrak{F}_R$. Then it follows from the second statement of Lemma 30 that a_i are also in $\mathcal{B}(\mathfrak{F}_R)$. Moreover in view of the inequality stated above, it is obvious that

$$|\,e^{t\rho(H)}\phi_a(\exp tH;b)$$
$$-\sum_{1\leqq i\leqq r} f_{a_i}(\exp tH;\mu_0(b))e^{t\rho(H)}\,| \leqq ce^{-t/t_0}\int(1+\|\lambda\|)^k\,|\,a(\lambda)\,|\,d\lambda$$

for $H \in V$ and $t \geqq 0$. On the other hand we can choose $d_0 \in S(\mathfrak{h}_\mathfrak{p})$ such that

$$c(1+t)^s e^{-t/t_0} \int (1+\|\lambda\|)^k |a(\lambda)|\, d\lambda \leqq \sup_{\lambda \in \mathfrak{F}_R} |d_0(\lambda) a(\lambda)|$$

for $t \geqq 0$ and $a \in \mathcal{B}(\mathfrak{F}_R)$. Furthermore

$$(1+t)^s e^{t\rho(H)} |f_{a_i}(\exp tH; \mu_0(b))| \leqq \sum_{1 \leqq j \leqq p} \sup_{\lambda \in \mathfrak{F}_R} |a(\lambda; d_j')|$$

for $H \in V$ and $t \geqq 0$ and, in view of the second statement of Lemma 30, we can select $d_1, \cdots, d_N \in \mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that

$$\sum_{1 \leqq i \leqq r} \sum_{1 \leqq j \leqq p} \sup_{\lambda \in \mathfrak{F}_R} |a_i(\lambda; d_j')| \leqq \sum_{1 \leqq i \leqq N} \sup_{\lambda \in \mathfrak{F}_R} |a(\lambda; d_i)|$$

for $a \in \mathcal{B}(\mathfrak{F}_R)$. Therefore the assertion of Lemma 38 is now obvious. This completes the proof of Theorem 3.

13. The distribution T_μ. Let dx denote the Haar measure on G.

LEMMA 39. *Fix an element μ in $\mathfrak{F}_R$. Then for any $a \in \mathcal{B}(\mathfrak{F}_R)$, the integral*

$$\int_G (\operatorname{conj} \phi(\mu : x)) \phi_a(x)\, dx$$

is well defined and the mapping

$$T_\mu : a \to \int (\operatorname{conj} \phi(\mu : x)) \phi_a(x)\, dx \qquad (a \in \mathcal{B}(\mathfrak{F}_R))$$

is a $\mathcal{B}$-distribution on $\mathfrak{F}_R$.

This is an immediate consequence of Theorem 3 and the following result.

LEMMA 40. *Let $f \in I(G)$, $\mu \in \mathfrak{F}_R$ and $b_1, b_2 \in \mathfrak{B}$. Then the integral*

$$\int_G |\phi(\mu : xy; b_1) f(x; b_2)|\, dx \qquad (y \in G)$$

converges uniformly with respect to y on every compact subset of G. Moreover the mapping

$$f \to \int_G |\phi(\mu : x; b_1) f(x; b_2)|\, dx \qquad (f \in I(G))$$

is continuous on $I(G)$.

From Lemma 46 of [2(i)] we can select a positive number c_1 such that $|\phi(\mu : x; b_1)| \leqq c_1 \phi(0 : x)$ for $x \in G$. Moreover if Ω is a compact subset of G, there exists a positive number c_2 such that $\phi(0 : xy) \leqq c_2 \phi(0 : x)$ for

$x \in G$ and $y \in \Omega$ (see [2(i), Lemma 48]). Therefore it would be sufficient to prove that

$$\int |\phi(0:x)f(x;b_2)|\,dx < \infty$$

and the mapping

$$f \to \int |\phi(0:x)f(x;b_2)|\,dx \qquad (f \in I(G))$$

is continuous on $I(G)$. Put $\Delta(\exp H) = \prod_{\alpha \in P_+} (e^{\alpha(H)} - e^{-\alpha(H)})$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$ as in [2(i), § 5]. Then if the Haar measure dh on $A_{\mathfrak{p}}$ is suitably normalized, we have

$$\int g(x)\,dx = \int_{A_{\mathfrak{p}^+}} \Delta(h)\,dh \int_{K\times K} g(k_1 h k_2)\,dk_1 dk_2$$

for any $g \in C_c(G)$ (see [2(f), § 12]). Therefore

$$\int |\phi(0:x)f(x;b_2)|\,dx = \int_{A_{\mathfrak{p}^+}} \Delta(h)\phi(0:h)\,dh \int_K |f(h;b_2{}^k)|\,dk.$$

We can obviously select a finite number of linearly independent elements $b_3, \cdots, b_N$ in $\mathfrak{B}$ and analytic functions $g_3, \cdots, g_N$ on K such that $b_2{}^k = \sum_{3 \leqq i \leqq N} g_i(k) b_i$ $(k \in K)$. Then

$$|f(h;b_2{}^k)| \leqq \sum_{3 \leqq i \leqq N} |g_i(k)|\,|f(h;b_i)|.$$

Since K is compact, the g_i remain bounded on K and so it would be sufficient to verify that for any $b \in \mathfrak{B}$,

$$\int_{A_{\mathfrak{p}^+}} \Delta(h)\phi(0:h)\,|f(h;b)|\,dh < \infty$$

and the mapping

$$f \to \int_{A_{\mathfrak{p}^+}} \Delta(h)\phi(0:h)\,|f(h;b)|\,dh \qquad (f \in I(G))$$

is continuous on $I(G)$. Choose an integer $q_1 \geqq 0$ such that

$$\int_{A_{\mathfrak{p}}} (1 + \|\log h\|)^{-q_1}\,dh < \infty$$

Since $|\Delta(h)|^{\frac{1}{2}} e^{-\rho(\log h)}$ obviously remains bounded for $h \in A_{\mathfrak{p}^+}$, we can, from Theorem 3 of [2(i)], select an integer $q_2 \geqq 0$ such that

$$(1 + \|\log h\|)^{-q_2} |\Delta(h)|^{\frac{1}{2}} \phi(0:h)$$

is bounded on $A_{\mathfrak{p}^+}$. On the other hand it follows from the definition

of D that $|\Delta(h)|^{\frac{1}{2}}(1+\|\log h\|)^{-q_3}D(h)^{-1}$ remains bounded on $A_\mathfrak{p}$ for a suitable integer $q_3 \geqq 0$. Hence there exists a positive number c such that $\Delta(h)\phi(0:h) \leqq cD_{q_2+q_3}(h)$ for $h \in A_\mathfrak{p}^+$. Therefore if we put $q = q_1 + q_2 + q_3$, it is clear that

$$\int_{A_\mathfrak{p}^+} \Delta(h)\phi(0:h)\,|f(h;b)|\,dh \leqq c\tau_{b,q}(f) \int_{A_\mathfrak{p}} (1+\|\log h\|)^{-q_1}\,dh$$

in the notation of Section 12. This proves our assertion.

COROLLARY 1. *Let Ω be a compact subset of $G \times G$. Then if $f \in I(G)$, the integral $\int_G |\phi(\mu:xy;b_1)f(xz;b_2)|\,dx$ converges uniformly for $(y,z) \in \Omega$.*

Without loss of generality we may assume that $\Omega = \omega_1 \times \omega_2$ where ω_1, ω_2 are compact subsets of G. Let ω be the image of Ω in G under the mapping $(y,z) \to z^{-1}y$. Then ω is also compact. Given any $\epsilon > 0$ we can, by Lemma 40, select a compact set V in G such that

$$\int_{{}^cV} |\phi(\mu:xy;b_1)f(x;b_2)|\,dx < \epsilon$$

for $y \in \omega$. (As usual ${}^cV$ denotes the complement of V in G.) Put $U = V\omega_2^{-1}$. Then U is also compact and ${}^cUz \subset {}^cV$ for $z \in \omega_2$. Hence if $y \in \omega_1$ and $z \in \omega_2$, it is clear that

$$\int_{{}^cU} |\phi(\mu:xy;b_1)f(xz;b_2)|\,dx = \int_{{}^cUz} |\phi(\mu:xz^{-1}y;b_1)f(x;b_2)|\,dx < \epsilon$$

from the right-invariance of the measure dx. This proves the corollary.

Now put

$$F(y:z) = \int_G \{\mathrm{conj}\,\phi(\mu:xy)\}f(xz)\,dx \qquad (y,z \in G).$$

Then the above corollary implies that F is a C^∞-function on $G \times G$ and

$$F(y;b_1:z;b_2) = \int_G (\mathrm{conj}\,\phi(\mu:xy;b_1))f(xz;b_2)\,dx$$

for $b_1, b_2 \in \mathfrak{B}$. On the other hand $F(y;b_1:z;b_2) = F(z^{-1}y;b_1:1;b_2)$ by the right-invariance of dx. Hence if we put $y = 1$ and $z = \exp tX$ $(X \in \mathfrak{g}_0, t \in R)$ and differentiate with respect to t at $t = 0$, we get $F(1;b_1:1;Xb_2) = -F(1;Xb_1:1;b_2)$. Let $b \to b^*$ denote the anti-automorphism of $\mathfrak{B}$ over R such that $(X + (-1)^{\frac{1}{2}}Y)^* = -X + (-1)^{\frac{1}{2}}Y$ $(X, Y \in \mathfrak{g}_0)$. Then the above result obviously implies the following corollary.

COROLLARY 2. *For any $b \in \mathfrak{B}$, $f \in I(G)$ and $\mu \in \mathfrak{F}_R$,*

$$\int_G (\mathrm{conj}\,\phi(\mu:x))f(x;b)\,dx = \int_G (\mathrm{conj}\,\phi(\mu:x;b^*))f(x)\,dx.$$

Moreover since $|\phi(\mu:x)| \leqq \phi(0:x)$ and the integral $\int \phi(0:x)|f(x)|\,dx$ is convergent, the following result is also obvious.

COROLLARY 3. *Fix an element $f \in I(G)$. Then the mapping*

$$\mu \to \int_G (\operatorname{conj} \phi(\mu:x))f(x)\,dx \qquad (\mu \in \mathfrak{F}_R)$$

is continuous on $\mathfrak{F}_R$.

We shall now try to determine the distribution T_μ of Lemma 39 explicitly. Define the homomorphism γ of $I_\mathfrak{g}$ into $I(\mathfrak{h}_\mathfrak{p})$ as in Section 4. Then we know from Lemma 18 of [2(i)] that $\phi(\lambda:x;q) = \gamma(q:(-1)^{\frac{1}{2}}\lambda)\phi(\lambda:x)$ $(x \in G, q \in I_\mathfrak{g}, \lambda \in \mathfrak{F})$. Let p_q denote the polynomial function on $\mathfrak{F}$ whose value at λ is $\gamma(q:(-1)^{\frac{1}{2}}\lambda)$. Then it follows from Theorem 3 that $q\phi_a = \phi_{p_q a}$ for $a \in \mathcal{B}(\mathfrak{F}_R)$ and we conclude from Corollary 2 of Lemma 40 that

$$T_\mu(p_q a) = \int (\operatorname{conj} \phi(\mu:x))\phi_a(x;q)\,dx = \int (\operatorname{conj} \phi(\mu:x;q^*))\phi_a(x)\,dx.$$

On the other hand $\operatorname{conj} \phi(\mu:x) = \phi(\mu:x^{-1})$ (see [2(i), Lemma 47]). Therefore it is obvious that $\operatorname{conj} \phi(\mu:1;b^*) = \phi(\mu:1;b)$ for any $b \in \mathfrak{B}$. On the other hand if b lies in $I_\mathfrak{g}$, the same holds for b^* and $\phi(\mu:1;b) = \gamma(b:(-1)^{\frac{1}{2}}\mu)$. Therefore

$$\operatorname{conj} \gamma(q^*:(-1)^{\frac{1}{2}}\mu) = \operatorname{conj} \phi(\mu:1;q^*) = \phi(\mu:1;q) = \gamma(q:(-1)^{\frac{1}{2}}\mu).$$

This proves that $T_\mu(p_q a) = p_q(\mu)T_\mu(a)$. Now let p be any element in $I(\mathfrak{h}_\mathfrak{p})$. Then by Theorem 1 of [2(i)], $p = p_q$ for some $q \in I_\mathfrak{g}$ and so we get the following result.

LEMMA 41. *$pT_\mu = p(\mu)T_\mu$ for any $p \in I(\mathfrak{h}_\mathfrak{p})$ and $\mu \in \mathfrak{F}_R$.*

COROLLARY. *There exists a continuous function $\mathfrak{B}$ on $\mathfrak{F}_R$ such that*

$$\pi_0(\mu)T_\mu(a) = \mathfrak{B}(\mu) \sum_{s \in W} \epsilon_0(s)a(s\mu)$$

for all $a \in \mathcal{B}(\mathfrak{F}_R)$ and $\mu \in \mathfrak{F}_R$. Moreover $\mathfrak{B}$ is unique and $\mathfrak{B}(s\mu) = \mathfrak{B}(\mu)$ $(s \in W)$.

Fix a point $\mu_0 \in \mathfrak{F}_R$. Then if $\mu \in \mathfrak{F}_R$ and $\mu \neq s\mu_0$ for any $s \in W$, it is clear that we can choose $p_0 \in I(\mathfrak{h}_\mathfrak{p})$ such that $p_0(\mu) \neq p_0(\mu_0)$. Put $p = p_0 - p_0(\mu_0)$. Then it follows from Lemma 41 that $pT_{\mu_0} = 0$. On the other hand $p(\mu) \neq 0$ and so we conclude that μ does not lie in the carrier of T_{μ_0}. This shows that this carrier is contained in the finite set of points $s\mu_0$ $(s \in W)$.

For any function a on $\mathfrak{F}_R$ and $s \in W$ define the function a^s by $a^s(\lambda) = a(s^{-1}\lambda)$ $(\lambda \in \mathfrak{F}_R)$. Then if $a \in \mathcal{C}(\mathfrak{F}_R)$, it is obvious that a^s also lies in $\mathcal{C}(\mathfrak{F}_R)$ and $\phi_{a^s} = \epsilon_0(s)\phi_a$. Hence $T_\mu(a^s) = \epsilon_0(s)T_\mu(a)$. Also $T_\mu = T_{s\mu}$ since $\phi_{s\mu} = \phi_\mu$ (see the corollary of Lemma 17 of [2(i)]). Let U be an open neighborhood of μ_0 in $\mathfrak{F}_R$ such that its closure is compact and $sU = U$ $(s \in W)$. Select a function $a_0 \in C_c^\infty(\mathfrak{F}_R)$ such that $a_0 = 1$ on U. Then if $\mu \in U$, it is clear that $\sum_{s \in W} \epsilon_0(s)\pi_0(s\mu)a_0(s\mu) = w\pi_0(\mu)$ where w is the order of W. Hence the uniqueness of $\boldsymbol{\beta}$ follows from its continuity and the equation $\pi_0(\mu)T_\mu(\pi_0 a_0) = w\boldsymbol{\beta}(\mu)\pi_0(\mu)$ $(\mu \in U)$. Therefore $\boldsymbol{\beta}(s\mu) = \boldsymbol{\beta}(\mu)$ since $T_{s\mu} = T_\mu$. Thus only the existence of $\boldsymbol{\beta}$ requires proof. Fix an integer $k \geqq 0$. Then for any given $a \in \mathcal{C}(\mathfrak{F}_R)$ and $\mu \in U$, we can select a polynomial $p \in S(\mathfrak{h}_\mathfrak{p})$ such that all derivatives of $a - p$ of order $\leqq k$ are zero at the points $s\mu$ $(s \in W)$. Hence if k is chosen sufficiently large, $T_\mu(a) = T_\mu(pa_0)$ (see Schwartz [4, p. 99]). But $a_0{}^s - a_0$ is identically zero on U and so it is obvious that $T_\mu(pa_0) = \epsilon_0(s)T_\mu(p^s a_0)$. Hence $T_\mu(a) = T_\mu(qa_0)$ where $q = w^{-1}\sum_{s \in W} \epsilon_0(s)p^s$. But from Lemma 32 we can choose $p_0 \in I(\mathfrak{h}_\mathfrak{p})$, such that $q = \pi_0 p_0$. Therefore

$$T_\mu(a) = T_\mu(p_0\pi_0 a_0) = p_0(\mu)T_\mu(\pi_0 a_0) \qquad (\mu \in U).$$

from Lemma 41. On the other hand $\pi_0(\mu)p_0(\mu) = q(\mu) = w^{-1}\sum_{s \in W} \epsilon_0(s)p(s\mu)$ $= w^{-1}\sum_{s \in W} \epsilon_0(s)a(s\mu)$. Therefore

$$\pi_0(\mu)T_\mu(a) = w^{-1}T_\mu(\pi_0 a_0)\sum_{s \in W} \epsilon_0(s)a(s\mu) \qquad (\mu \in U).$$

But from Corollary 3 of Lemma 40, $T_\mu(\pi_0 a_0)$ is a continuous function of μ and so our assertion is proved.

Define $\boldsymbol{b}_0$ as in Section 9. We shall see in Section 15 that if the measure $d\lambda$ on $\mathfrak{F}_R$ is suitably normalized, $\boldsymbol{\beta}(\lambda) = |\boldsymbol{b}_0(\lambda)|^2$ for $\lambda \in \mathfrak{F}_R$. This, in fact, is one of the main results of this paper.

14. An inequality and its consequences. Put $\mathfrak{n} = \sum_{\alpha \in P_+} CX_\alpha$ as in [2(i), § 2] and $\bar{\mathfrak{n}} = \theta\mathfrak{n} = \sum_{\alpha \in P_+} CX_{-\alpha}$ where θ is the automorphism of $\mathfrak{g}$ defined in Section 2. Let N and $\bar{N}$ be the analytic subgroups of G corresponding to $\mathfrak{n} \cap \mathfrak{g}_0$ and $\bar{\mathfrak{n}} \cap \mathfrak{g}_0$ respectively. We normalize their Haar measures dn and $d\bar{n}$ in such a way (see [2(i), Lemma 44]) that

$$\int_N e^{-2\rho(H(n'))}dn = \int_{\bar{N}} e^{-2\rho(H(\bar{n}))}d\bar{n} = 1$$

where $n' = \theta(n^{-1})$ $(n \in N)$.

LEMMA 42. *Let h and $\bar{n}$ be two elements in $A_\mathfrak{p}$ and $\bar{N}$ respectively and select $h' \in \mathrm{Cl}(A_\mathfrak{p}^+)$ such that $\bar{n}h \in Kh'K$. Then $\rho(\log h') \geqq \rho(H(\bar{n})) + \rho(\log h)$ and therefore $\| \log h' \| \geqq \| \rho \|^{-1}\{\rho(H(\bar{n})) + \rho(\log h)\}$.*

Put $\Lambda = \frac{1}{2}\sum_{\alpha \in P} \alpha$ and let σ denote the irreducible representation of $\mathfrak{g}$ on a finite-dimensional space V with the highest weight Λ (see the proof of Lemma 45 of [2(i)]). Choose a unit vector ψ_0 in V belonging to the weight Λ. Then if $\bar{n}h = k_1 h' k_2$ $(k_1, k_2 \in K)$, it follows that $|\sigma(\bar{n}h)\psi_0| = |\sigma(h'k_2)\psi_0|$. But since Λ coincides with ρ on $\mathfrak{h}_\mathfrak{p}$, this shows that $\rho(H(\bar{n})) + \rho(\log h) = \rho(H(h'k_2))$. However $h' \in \mathrm{Cl}(A_\mathfrak{p}^+)$ and therefore we conclude from Corollary 3 of Lemma 35 of [2(i)] that $\rho(H(h'k_2)) \leqq \rho(\log h')$. Hence the lemma.

COROLLARY 1. *Let Ω be a subset of $A_\mathfrak{p}$ such that $\rho(\log h)$ remains bounded from below as h varies in Ω. Then for any integer $k \geqq 0$, we can select a positive number c_1 and an integer $k_1 \geqq 0$ such that*

$$D_{k_1}(\bar{n}h) \geqq c_1\{1 + \rho(H(\bar{n}))\}^k \exp\{\rho(H(\bar{n})) + |\rho(\log h)|\}$$

for all $\bar{n} \in \bar{N}$ and $h \in \Omega$.

It is easily seen that we can select an integer $d \geqq 0$ and a positive number c_2 such that $D(h_0)e^{-\rho(\log h_0)}(1 + \| \log h_0 \|)^d \geqq c_2$ for $h_0 \in \mathrm{Cl}(A_\mathfrak{p}^+)$. Therefore if h' is defined as above, it follows that

$$D_d(\bar{n}h) = D_d(h') \geqq c_2 e^{\rho(\log h')} \geqq c_2 \exp\{\rho(H(\bar{n})) + \rho(\log h)\}.$$

Hence in view of Lemma 42 and our assumption on Ω, the statement of the corollary is obvious.

COROLLARY 2. *Let U be a compact subset of $\bar{N}$ and fix f and b in $I(G)$ and $\mathfrak{B}$ respectively. Then the integral $\int_{\bar{N}} |f(\bar{n}\bar{n}_0 h; b)|\, d\bar{n}$ converges uniformly as $\bar{n}_0$ and h vary in U and Ω respectively. Moreover, we can find an integer $r \geqq 0$ and a positive number c such that*

$$\int_{\bar{N}} |f(\bar{n}h; b)|\, d\bar{n} \leqq c \sup_{x \in G} D_r(x)\, |f(x; b)|$$

for all $h \in \Omega$, $f \in I(G)$ and $b \in \mathfrak{B}$.

From Lemma 45 of [2(i)], we can select an integer $k \geqq 0$ so large that

$$c_2 = \int_{\bar{N}} \{1 + \rho(H(\bar{n}))\}^{-k} e^{-\rho(H(\bar{n}))} d\bar{n} < \infty.$$

Choose k_1 and c_1 corresponding to Corollary 1 above. Then

$$|f(\bar{n}h;b)| \leqq c_1^{-1}\tau_b(f)e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k}$$

for $\bar{n} \in \bar{N}$, $h \in \Omega$, $b \in \mathfrak{B}$ and $f \in I(G)$, where

$$\tau_b(f) = \sup_{x \in G} D_{k_1}(x)|f(x;b)|.$$

Hence it is sufficient to choose $r = k_1$ and $c = c_1^{-1}c_2$. Moreover for any $\epsilon > 0$, we can select a compact set V_0 in $\bar{N}$ such that

$$\int_{{}^cV_0} \{1+\rho(H(\bar{n}))\}^{-k}e^{-\rho(N(\bar{n}))}d\bar{n} < \epsilon.$$

(${}^cV_0$ is the complement of V_0 in $\bar{N}$.) Put $V = V_0U^{-1}$. Then V is also compact and

$$\int_{{}^cV} \{1+\rho(H(\bar{n}\bar{n}_0))\}^{-k}\exp\{-\rho(H(\bar{n}\bar{n}_0))\}d\bar{n} < \epsilon$$

for $\bar{n}_0 \in U$. From this the first assertion of the corollary follows immediately.

Put $\bar{\mathfrak{N}}_1 = \bar{\mathfrak{N}}\bar{\mathfrak{n}}$ where $\bar{\mathfrak{N}}$ is the subalgebra of $\mathfrak{B}$ generated by $(1, \bar{\mathfrak{n}})$. Moreover for any function F on G write $F(\bar{n}:h) = F(\bar{n}h)$ $(\bar{n} \in \bar{N}, h \in A_\mathfrak{p})$.

COROLLARY 3. *Suppose* $\eta \in \bar{\mathfrak{N}}_1$ *and* $u \in \mathfrak{H}_\mathfrak{p}$. *Then*

$$\int_{\bar{N}} f(\bar{n};\eta:h;u)\,d\bar{n} = 0$$

for $f \in I(G)$ *and* $h \in A_\mathfrak{p}$.

Fix h and put $\eta' = (\eta)^{h^{-1}}$ for any $\eta \in \bar{\mathfrak{N}}$. Then $f(\bar{n};\eta:h;u) = f(\bar{n}h;\eta'u)$ and therefore, by Corollary 2, the integral

$$\int_{\bar{N}} |f(\bar{n}\bar{n}_0;\eta:h;u)|\,d\bar{n}$$

converges uniformly as $\bar{n}_0$ varies within a compact subset of $\bar{N}$. Put

$$F(\bar{n}_0) = \int f(\bar{n}\bar{n}_0;\eta:h;u)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}).$$

Then it follows from the above remarks that F is of class C^∞ on $\bar{N}$ and

$$F(\bar{n}_0;\eta_1) = \int f(\bar{n}\bar{n}_0;\eta_1\eta:h;u)\,d\bar{n}$$

for $\eta_1 \in \bar{\mathfrak{N}}$. However the Haar measure on the nilpotent group $\bar{N}$ is both

left- and right-invariant. Therefore $F(\bar{n}_0) = F(1)$ and hence $F(\bar{n}_0; X) = 0$ for $X \in \bar{\mathfrak{n}}$. This shows that

$$\int f(\bar{n}; X\eta : h; u)\, d\bar{n} = 0$$

for $X \in \bar{\mathfrak{n}}$ and $\eta \in \mathfrak{N}$ and now our assertion is obvious.

Let $\mathcal{B}(A_\mathfrak{p})$ denote the set of all functions F on $A_\mathfrak{p}$ of class C^∞ such that

$$\sigma_{q,u}(F) = \sup_{h \in A_\mathfrak{p}} (1 + \| \log h \|)^q \, | F(h; u) | < \infty$$

for any integer $q \geqq 0$ and $u \in \mathfrak{H}_\mathfrak{p}$. We define a topology in $\mathcal{B}(A_\mathfrak{p})$ by means of the seminorms $\sigma_{q,u}$ and thus turn it into a locally convex space. Let $I(A_\mathfrak{p})$ denote the subspace of $\mathcal{B}(A_\mathfrak{p})$ consisting of those elements which are invariant under W. Obviously $I(A_\mathfrak{p})$ is closed in $\mathcal{B}(A_\mathfrak{p})$.

COROLLARY 4. *For any $f \in I(G)$, put $F_f(h) = e^{\rho(\log h)} \int_{\bar{N}} f(\bar{n}h)\, d\bar{n}$ $(h \in A_\mathfrak{p})$. Then $F_f \in I(A_\mathfrak{p})$ and $f \to F_f$ is a continuous mapping of $I(G)$ into $I(A_\mathfrak{p})$. Moreover*

$$F_f(h; u) = e^{\rho(\log h)} \int_{\bar{N}} f(\bar{n}h; u')\, d\bar{n} \qquad (h \in A_\mathfrak{p}, u \in \mathfrak{H}_\mathfrak{p})$$

where $u' = e^{-\rho} u \circ e^{\rho}$.

It is obvious from Corollary 2 that F_f is of class C^∞ and

$$F_f(h; u) = e^{\rho(\log h)} \int_{\bar{N}} f(\bar{n}h; u')\, d\bar{n}$$

for $u \in \mathfrak{H}_\mathfrak{p}$. Moreover $f(x) = f(\theta(x^{-1}))$ $(x \in G)$, since f is spherical. Therefore

$$F_f(h) = e^{\rho(\log h)} \int_N f(hn)\, dn.$$

We can now apply to f the proof of Lemma 17 of [2(i)] and conclude that $F_f(h^s) = F_f(h)$ $(s \in W)$.

Select k as in the proof of Corollary 2. Since $\rho(\log h) \geqq 0$ for $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$, we can take $\Omega = \mathrm{Cl}(A_\mathfrak{p}^+)$. Now choose k_1 as in Corollary 1. Then it is obvious from Lemma 42, that for any integer $q \geqq 0$, there exists a positive constant c_q such that

$$D_{k_1+q}(\bar{n}h) \geqq c_q (1 + \| \log h \|)^q \{1 + \rho(H(\bar{n}))\}^k \exp\{\rho(\log h) + \rho(H(\bar{n}))\}$$

for $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$ and $\bar{n} \in \bar{N}$. This shows that

$$(1 + \| \log h \|)^q \, | F_f(h; u) | \leqq c c_q^{-1} \sup_{x \in G} D_{k_1+q}(x) \, | f(x; u') |$$

for $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$, $u \in \mathfrak{H}_{\mathfrak{p}}$ and $f \in I(G)$, where

$$c = \int_{\bar{N}} e^{-\rho(H(\bar{n}))}\{1 + \rho(H(\bar{n}))\}^{-k}\, d\bar{n}.$$

Let $u \to u^s$ $(s \in W)$ denote the automorphism of $\mathfrak{H}_{\mathfrak{p}}$ which coincides with s on $\mathfrak{h}_{\mathfrak{p}}$. Then obviously $F_f(h\,;u) = F_f(h^s\,;u^s)$. Therefore since $A_{\mathfrak{p}} = \bigcup_{s \in W} s(\mathrm{Cl}(A_{\mathfrak{p}}^+))$, it follows that

$$\sup_{h \in A_{\mathfrak{p}}} (1 + \| \log h \|)^q \,|\, F_f(h\,;u)| \leqq cc_q^{-1} \sum_{s \in W} \sup_{x \in G} D_{k_1+q}(x)\,|\, f(x\,;\,(u^s)')|$$

for $f \in I(G)$, $u \in \mathfrak{H}_{\mathfrak{p}}$ and $q \geqq 0$. This proves the corollary.

We normalize the Haar measure dh on $A_{\mathfrak{p}}$ in such a way (see [2(b), Lemma 35]) that $dx = e^{2\rho(\log h)} dk\,dh\,dn$ for $x = khn$ $(k \in K, h \in A_{\mathfrak{p}}, n \in N)$.

LEMMA 43. *For any $\lambda \in \mathfrak{F}_R$ and $f \in I(G)$,*

$$\int_G \phi_\lambda(x) f(x)\, dx = \int_{A_{\mathfrak{p}}} F_f(h) \exp\{(-1)^{\frac{1}{2}} \lambda(\log h)\}\, dh.$$

We keep to the notation of the proof of Corollary 4 of Lemma 42. Select an integer $q \geqq 0$ so large that $\int_{A_{\mathfrak{p}}} (1 + \| \log h \|)^{-q}\, dh < \infty$. Fix $f \in I(G)$ and put

$$g(h) = e^{\rho(\log h)} \int_N |\, f(hn)|\, dn = e^{\rho(\log h)} \int_{\bar{N}} |\, f(\bar{n}h)|\, d\bar{n}$$

for $h \in A_{\mathfrak{p}}$. One proves without difficulty (see [2(i), Lemma 17]) that $g(h^s) = g(h)$ for $s \in W$. Hence

$$\int_G |\, f(x)|\, e^{-\rho(H(x))} dx = \int_{A_{\mathfrak{p}}} g(h)\, dh = w \int_{A_{\mathfrak{p}}^+} g(h)\, dh$$

where w is the order of W. On the other hand

$$e^{-\rho(H(\bar{n}))}\{1 + \rho(H(\bar{n}))\}^{-k} \sup_{x \in G} D_{k_1+q}(x)\,|\, f(x)|$$
$$\geqq c_q (1 + \| \log h \|)^q e^{\rho(\log h)}\,|\, f(\bar{n}h)|$$

for $\bar{n} \in \bar{N}$ and $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$ and therefore

$$g(h) \leqq cc_q^{-1} (1 + \| \log h \|)^{-q} \sup_{x \in G} D_{k_1+q}(x)\,|\, f(x)| \qquad (h \in A_{\mathfrak{p}}^+).$$

This shows that $\int |\, f(x)|\, e^{-\rho(H(x))} dx < \infty$. Hence it follows immediately

that

$$\int_G \phi_\lambda(x)f(x)dx = \int_G f(x)\exp\{(-1)^{\frac{1}{2}}\lambda(H(x)) - \rho(H(x))\}dx$$
$$= \int_{A_\mathfrak{p}} \exp\{(-1)^{\frac{1}{2}}\lambda(\log h) + \rho(\log h)\}dh \int_N f(hn)dn$$
$$= \int_{A_\mathfrak{p}} F_f(h)\exp\{(-1)^{\frac{1}{2}}\lambda(\log h)\}dh.$$

Let us now assume that $d\lambda$ is the *regular* Euclidean measure (see [2(g), §2]) on $\mathfrak{F}_R$ and the Haar measure dh on $A_\mathfrak{p}$ is so normalized that

$$\int_{A_\mathfrak{p}} dh \int_{\mathfrak{F}_R} a(\lambda)\exp\{(-1)^{\frac{1}{2}}\lambda(\log h)\}d\lambda = a(0)$$

for any $a \in \mathcal{B}(\mathfrak{F}_R)$. In view of the relation $dx = e^{2\rho(\log h)}dkdhdn$, this fixes the normalization of dx as well. We shall call these the regular normalizations of $d\lambda$, dx and dh. Define $\mathfrak{B}$ as in the corollary of Lemma 41.

COROLLARY. *Let a be any element in $\mathcal{B}(\mathfrak{F}_R)$. Then*

$$e^{\rho(H)}\int_{\bar{N}} \phi_a(\bar{n}\exp H)\,d\bar{n} = \int_{\mathfrak{F}_R} \mathfrak{B}(\lambda)\{\pi_0(\lambda)^{-1}\sum_{s\in W}\epsilon_0(s)a(s\lambda)\}e^{(-1)^{\frac{1}{2}}\lambda(H)}\,d\lambda$$

for $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

Put $f = \phi_a$. Then from Theorem 3, f lies in $I(G)$ and therefore by Lemma 43,

$$\int F_f(h)\exp\{-(-1)^{\frac{1}{2}}\lambda(\log h)\}dh = \int \phi_a(x)\,\mathrm{conj}\,\phi_\lambda(x)\,dx \quad (\lambda \in \mathfrak{F}_R).$$

Now apply the corollary of Lemma 41. Then

$$\pi_0(\lambda)\int F_f(h)\exp\{-(-1)^{\frac{1}{2}}\lambda(\log h)\}dh = \mathfrak{B}(\lambda)\sum_{s\in W}\epsilon_0(s)a(s\lambda).$$

Therefore our assertion follows immediately by the Fourier inversion formula.

We shall see in the next section that the above relation also holds if $\mathfrak{B}(\lambda)$ is replaced by $|\boldsymbol{b}_0(\lambda)|^2$. This would prove that $\mathfrak{B}(\lambda) = |\boldsymbol{b}_0(\lambda)|^2$ for $\lambda \in \mathfrak{F}_R$.

15. Determination of the function $\mathfrak{B}$. Extend θ to an automorphism of $\mathfrak{B}$ and put $\mathfrak{N} = \theta(\bar{\mathfrak{N}})$, $\mathfrak{N}_1 = \theta(\bar{\mathfrak{N}}_1)$ and $\gamma'(q) = e^{-\rho}\gamma(q)\circ e^{\rho}$ $(q \in I_\mathfrak{g})$. Also define $\mathfrak{B}_d$ as in Lemma 9.

LEMMA 44. *Let q be an element in $I_\mathfrak{g}$ and let d denote the degree of $\gamma(q)$. Then $q - \gamma'(q) \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d$.*

Define $\mathfrak{P}$ as in Lemma 19 of [2(i)]. Then we have seen in [2(i), § 4] that $I_\mathfrak{g} = I_\mathfrak{g} \cap \mathfrak{P} + I_\mathfrak{g} \cap (\mathfrak{k}\mathfrak{B})$. On the other hand $I_\mathfrak{g} \cap (\mathfrak{k}\mathfrak{B}) = I_\mathfrak{g} \cap (\mathfrak{B}\mathfrak{k})$ is the kernel of γ (see [2(i), Theorem 1]). So it would be sufficient to consider the case when $q \in I_\mathfrak{g} \cap \mathfrak{P}$. But then it follows from [2(i), Lemma 20] that q itself is of degree d. Now $\mathfrak{g}$ is the direct sum of $\mathfrak{k}$, $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{n}$. Hence $\mathfrak{B}_d \subset \mathfrak{k}\mathfrak{B} + (\mathfrak{H}_\mathfrak{p}\mathfrak{N}) \cap \mathfrak{B}_d$ from [2(b), Lemma 12]. Therefore it follows from the definition of γ (see [2(i), § 4]) that $q - \gamma'(q) \in \mathfrak{k}\mathfrak{B} + (\mathfrak{H}_\mathfrak{p}\mathfrak{N}_1) \cap \mathfrak{B}_d$. Let $b \to b^\dagger$ ($b \in \mathfrak{B}$) denote the anti-automorphism of $\mathfrak{B}$ such that $X^\dagger = -\theta(X)$ ($X \in \mathfrak{g}$). It is clear that every element of $\mathfrak{p}$ (and therefore also of $\mathfrak{P}$) is left fixed by this anti-automorphism. Hence

$$q - \gamma'(q) = (q - \gamma'(q))^\dagger \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d.$$

This proves the lemma.

Select $u_1 = 1, u_2, \cdots, u_w \in \mathfrak{H}_\mathfrak{p}$ as in the corollary of Lemma 8 of [2(i)] and let $u \to u'$ denote the automorphism of $\mathfrak{H}_\mathfrak{p}$ given by $u' = e^{-\rho} u \circ e^\rho$ ($u \in \mathfrak{H}_\mathfrak{p}$).

LEMMA 45. *Suppose* $u = \sum_{1 \leqq i \leqq w} u_i \gamma(q_i)$ $(q_i \in I_\mathfrak{g})$. *Then we can choose a finite number of elements* $q_{ki} \in I_\mathfrak{g}$ *and* $\eta_{ki} \in \bar{\mathfrak{N}}_1$ $(1 \leqq k \leqq r,\ 1 \leqq i \leqq w)$ *such that*

$$u' \equiv \sum_{1 \leqq i \leqq w} u_i' q_i + \sum_{1 \leqq k \leqq r} \sum_{1 \leqq i \leqq w} \eta_{ki} u_i' q_{ki} \bmod \mathfrak{B}\mathfrak{k}.$$

We shall use induction on the degree d of u. Obviously we may assume that u is homogeneous and $d \geqq 1$. Then $u_i \gamma(q_i)$ $(1 \leqq i \leqq w)$ are also homogeneous of degree d (see the corollary of Lemma 8 of [2(i)]) and it follows from Lemma 44 that

$$\sum_i u_i' q_i - \sum_i u_i' \gamma'(q_i) \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d.$$

But this implies that

$$u' \equiv \sum_i u_i' q_i + \sum_{1 \leqq k \leqq s} \eta_k v_k' \bmod \mathfrak{B}\mathfrak{k}$$

where $\eta_k \in \bar{\mathfrak{N}}_1$ and $v_k \in \mathfrak{H}_\mathfrak{p} \cap \mathfrak{B}_{d-1}$ $(1 \leqq k \leqq s)$. On the other hand $\mathfrak{H}_\mathfrak{p} = \sum_{1 \leqq i \leqq w} J u_i$ where $J = I(\mathfrak{h}_\mathfrak{p}) = \gamma(I_\mathfrak{g})$. Therefore our assertion follows by applying the induction hypothesis to v_k.

Select $\alpha_1, \cdots, \alpha_l \in \Sigma$ as in [2(i), § 3] and consider the additive group L generated by Σ. Then $(\alpha_1, \cdots, \alpha_l)$ is a set of independent generators of L. We say that an element $b \in \mathfrak{B}$ is of rank β $(\beta \in L)$ if $[H, b] = Hb - bH = \beta(H)b$ for every $H \in \mathfrak{h}_\mathfrak{p}$. Let L_+ be the set of all elements $\beta \in L$ of the form $\beta = m_1\alpha_1 + \cdots + m_l\alpha_l$ where $m_1, \cdots, m_l$ are nonnegative integers

which are not all zero. Let $(\bar{\mathfrak{N}}_1)_{-\beta}$ $(\beta \in L_+)$ denote the set of all elements in $\bar{\mathfrak{N}}_1$ of rank $-\beta$. Then it is easy to see that $\bar{\mathfrak{N}}_1$ is the direct sum of $(\bar{\mathfrak{N}}_1)_{-\beta}$ for $\beta \in L_+$. Therefore it is obvious that the elements η_{ki} of Lemma 45 can be so chosen that η_{ki} is of the rank $-\beta_{ki}$ for some $\beta_{ki} \in L_+$. Now we use the notation of Section 14.

COROLLARY. *Assume that η_{ki} is of rank $-\beta_{ki}$ $(\beta_{ki} \in L_+)$ in Lemma 45. Then*

$$\phi_\lambda(\bar{n}:h;u') = \sum_{1\leqq i\leqq w} \gamma(q_i:(-1)^{\frac{1}{2}}\lambda)\phi_\lambda(\bar{n}:h;u_i') + \sum_{1\leqq k\leqq r}\sum_{1\leqq i\leqq w} e^{-\beta_{ki}(\log h)}\gamma(q_{ki}:(-1)^{\frac{1}{2}}\lambda)\phi_\lambda(\bar{n};\eta_{ki}:h;u_i')$$

for $\lambda \in \mathfrak{F}$, $\bar{n} \in \bar{N}$ and $h \in A_{\mathfrak{p}}$.

It follows from Lemma 45 and [2(i), Lemma 18] that

$$\phi_\lambda(x;u') = \sum_i \gamma(q_i:(-1)^{\frac{1}{2}}\lambda)\phi_\lambda(x;u_i') + \sum_{k,i}\gamma(q_{ki}:(-1)^{\frac{1}{2}}\lambda)\phi_\lambda(x;\eta_{ki}u_i')$$

for $x \in G$. Now if we put $x = \bar{n}h$ and observe that

$$\phi_\lambda(\bar{n}h;\eta_{ki}u_i') = e^{-\beta_{ki}(\log h)}\phi_\lambda(\bar{n};\eta_{ki}:h;u_i'),$$

our assertion follows immediately.

Now put

$$\Phi_j(\lambda:\bar{n}:h:H) = \pi_0(\lambda)e^{\rho(\log h+H)}\phi_\lambda(\bar{n}:h\exp H;u_j') \qquad (1\leqq j\leqq w)$$

for $\lambda \in \mathfrak{F}$, $\bar{n} \in \bar{N}$, $h \in A_{\mathfrak{p}}$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Suppose $Hu_i = \sum_j u_j\gamma(q_{ji})$ where $q_{ji} \in I_{\mathfrak{g}}$. Then we put $\Xi_{ij}(\lambda:H) = \gamma(q_{ji}:(-1)^{\frac{1}{2}}\lambda)$ $(1\leqq i,j\leqq w)$. It is clear that $\Xi_{ij}(\lambda:H)$ depend on H but not on the particular choice of q_{ji}. Now fix an element $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}^+$. By Lemma 45 we can choose elements q_{ji}, q_{kji} in $I_{\mathfrak{g}}$ and η_{kij} in $\bar{\mathfrak{N}}_1$ $(1\leqq i,j\leqq w,\ 1\leqq k\leqq r)$ such that

$$H_0u_i' \equiv \sum_{1\leqq j\leqq w} u_j'q_{ji} + \sum_{1\leqq k\leqq r}\sum_{1\leqq j\leqq w}\eta_{kij}u_j'q_{kji} \bmod \mathfrak{B}\mathfrak{f} \qquad (1\leqq i\leqq w).$$

Moreover we may assume that η_{kij} is of rank $-\beta_{kij}$ for suitable $\beta_{kij} \in L_+$. Then it follows from the corollary of Lemma 45 that

$$d\Phi_i(\lambda:\bar{n}:h:tH_0)/dt = \sum_{1\leqq j\leqq w}\gamma(q_{ji}:(-1)^{\frac{1}{2}}\lambda)\Phi_j(\lambda:\bar{n}:h:tH_0) + \sum_{1\leqq k\leqq r}\sum_{1\leqq j\leqq w}\gamma(q_{kji}:(-1)^{\frac{1}{2}}\lambda)\Phi_j(\lambda:\bar{n};\eta_{kij}:h:tH_0) \times \exp\{-\beta_{kij}(\log h + tH_0)\}.$$

In matrix notation, this equation can be written as follows.

$$d\Phi(\lambda:\tilde{n}:h:tH_0)/dt = \Xi(\lambda:H_0)\Phi(\lambda:\tilde{n}:h:tH_0) + \Psi(\lambda:\tilde{n}:h:t)$$

where

$$\Psi_i(\lambda:\tilde{n}:h:t) = \sum_{1\leqq k\leqq r}\sum_{1\leqq j\leqq w}\gamma(q_{kji}:(-1)^{\frac{1}{2}}\lambda)\Phi_j(\lambda:\tilde{n};\eta_{kij}:h:tH_0) \times\exp\{-\beta_{kij}(\log h + tH_0)\}$$

$(1\leqq i\leqq w)$. Put $\Phi(\lambda:\tilde{n}:h:t) = \Phi(\lambda:\tilde{n}:h:tH_0), \Phi(\lambda:\tilde{n}:h) = \Phi(\lambda:\tilde{n}:h:0)$,

$$\Phi^0(\lambda:\tilde{n}:h:t) = \exp(-t\Xi(\lambda:H_0))\Phi(\lambda:\tilde{n}:h:t),$$
$$\Psi^0(\lambda:\tilde{n}:h:t) = \exp(-t\Xi(\lambda:H_0))\Psi(\lambda:\tilde{n}:h:t) \qquad (t\in R).$$

Then the following lemma is obvious.

LEMMA 46. *$d\Phi^0(\lambda:\tilde{n}:h:t)/dt = \Psi^0(\lambda:\tilde{n}:h:t)$ and therefore*

$$\Phi^0(\lambda:\tilde{n}:h:T) = \Phi(\lambda:\tilde{n}:h) + \int_0^T \Psi^0(\lambda:\tilde{n}:h:t)\,dt$$

for $T\geqq 0$.

Put $\beta = \min_{\alpha\in P_+}\alpha(H_0)$ and let ω denote a compact subset of $\mathfrak{F}_R$. It follows from Corollary 2 of Lemma 14 of [2(i)] that $(-1)^{\frac{1}{2}}\lambda(sH_0)$ $(s\in W)$ are all the eigenvalues of $\Xi(\lambda:H_0)$. Hence by Lemma 60 of [2(i)], there exists a positive number c_1 such that $\|\exp(-t\Xi(\lambda:H_0))\|\leqq c_1(1+t)^w$ for $t\geqq 0$ and $\lambda\in\omega$. Put $x^\dagger = \theta(x^{-1})$ as in Section 2 $(x\in G)$. Then $x^\dagger\in KxK$ and therefore $\phi_\lambda(x^\dagger) = \phi_\lambda(x)$. Let $b\to b^\dagger$ denote the anti-automorphism of $\mathfrak{B}$ such that $X^\dagger = -\theta(X)$ $(X\in\mathfrak{g})$. Then if $\eta\in\bar{\mathfrak{N}}$ and $u\in\mathfrak{S}_\mathfrak{p}$, it follows without difficulty that

$$\phi(\lambda:\tilde{n};\eta:h;u) = \phi_\lambda(hn;b)$$

where $n = (\tilde{n})^\dagger$ and $b = ((\eta u)^{\tilde{n}})^\dagger$. Therefore since $D(x)\geqq 1$ $(x\in G)$, we get the following result from Theorem 2.

LEMMA 47. *Let U and ω denote two compact subsets of $\bar{N}$ and $\mathfrak{F}_R$ respectively. Then for any $h\in A_\mathfrak{p}$, we can select a positive constant c such that*

$$\|\Psi^0(\lambda:\tilde{n}:h:t)\|\leqq c(1+t)^w e^{-\beta t}$$

for $\lambda\in\omega$, $\tilde{n}\in U$ and $t\geqq 0$.

It is obvious from Lemmas 46 and 47 that $\Phi^0(\lambda:\tilde{n}:h:t)$ tends to a limit as $t\to+\infty$ if $\lambda\in\mathfrak{F}_R$. We denote this limit by $\Phi^0(\lambda:\tilde{n}:h:\infty)$.

COROLLARY. *For a fixed h in $A_\mathfrak{p}$, $\Phi^0(\lambda:\bar{n}:h:\infty)$ is a continuous function of $(\lambda,\bar{n})$ on $\mathfrak{F}_R\times\bar{N}$.*

It follows from Lemma 47 that the integral $\int_0^\infty \|\Psi^0(\lambda:\bar{n}:h:t)\|\,dt$ converges uniformly as λ and $\bar{n}$ vary in ω and U respectively. The corollary is an immediate consequence of this fact.

As before let $\mathfrak{F}_R'$ be the set of those points λ in $\mathfrak{F}_R$ where $\pi(\lambda)\neq 0$. Fix an open subset ω of $\mathfrak{F}_R'$ such that its closure in $\mathfrak{F}_R'$ is compact. We also assume that $s\omega=\omega$ for $s\in W$. Select an element p in $S(\mathfrak{h}_\mathfrak{p})$ and for any $a\in C_c^\infty(\omega)$, put $a_t(\lambda)=a(\lambda)\pi(\lambda)^{-1}p(\lambda)\exp\{-(-1)^{\frac{1}{2}}t\lambda(H_0)\}$ $(t\in R,\lambda\in\mathfrak{F}_R)$. Obviously $a_t\in C_c^\infty(\omega)$ for any t. Now choose an integer $k_0\geqq 0$ such that

$$\int_{\bar{N}} e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}\,d\bar{n}<\infty.$$

LEMMA 48. *Define Ω as in Corollary 1 of Lemma 42 and let b be an element in $\mathfrak{B}$. Then there exists an integer $m\geqq 0$ with the following property. For any $a\in C_c^\infty(\omega)$, we can select a positive number c_a such that*

$$|\phi_{a_t}(\bar{n}h;b)|\leqq c_a(1+t)^m\exp\{-|\rho(\log h)|-\rho(H(\bar{n}))\}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for $\bar{n}\in\bar{N}$, $h\in\Omega$ and $t\geqq 0$.

From Corollary 1 of Lemma 42, we can choose an integer $k_1\geqq 0$ and a positive number c_1 such that

$$|f(\bar{n}h;b)|$$
$$\leqq c_1\exp\{-|\rho(\log h)|-\rho(H(\bar{n}))\}\{1+\rho(H(\bar{n}))\}^{-k_0}\sup_{x\in G}D_{k_1}(x)|f(x;b)|$$

for any $f\in I(G)$. On the other hand by Theorem 3 we can select a finite number of differential operators $d_1,\cdots,d_r$ in $\mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that

$$\sup_{x\in G}D_{k_1}(x)|\phi_a(x;b)|\leqq\sum_{1\leqq i\leqq r}\sup_{\lambda\in\omega}|a(\lambda;d_i)|$$

for $a\in C_c^\infty(\omega)$. Let m_i denote the order of d_i. Then if $m=\max(m_1,\cdots,m_r)$, it is obvious that for any $a\in C_c^\infty(\omega)$, there exists a positive constant c' such that

$$\sum_{1\leqq i\leqq r}\sup_{\lambda\in\omega}|a_t(\lambda;d_i)|\leqq c'(1+t)^m$$

for all $t\geqq 0$. From this our assertion follows immediately.

COROLLARY 1. *Let u be an element in $\mathfrak{H}_\mathfrak{p}$ and η an element in $\bar{\mathfrak{N}}_1$ of rank $-\beta_0$ $(\beta_0\in L_+)$. Then we can select an integer $m\geqq 0$ and, for any $a\in C_c^\infty(\omega)$ and $h\in A_\mathfrak{p}$, a positive constant $c(a,h)$ such that*

$$e^{\rho(\log h+tH_0)}\,|\,\phi_{a_t}(\bar{n}\,;\eta:h\exp tH_0\,;u)\,|\,e^{-\beta_0(\log h+tH_0)}$$
$$\leqq c(a,h)(1+t)^m e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for $\bar{n}\in\bar{N}$ *and* $t\geqq 0$.

This is obvious from the above lemma if we note that

$$\phi_{a_t}(\bar{n}\,;\eta:h\exp tH_0\,;u)\,e^{-\beta_0(\log h+tH_0)}=\phi_{a_t}(\bar{n}h\exp tH_0\,;\eta u).$$

For any $a\in C_c^\infty(\omega)$, put

$$\Phi^0(a:\bar{n}:h:t)=\int_{\mathfrak{F}_R}a(\lambda)\Phi^0(\lambda:\bar{n}:h:t)\,d\lambda,$$
$$\Psi^0(a:\bar{n}:h:t)=\int_{\mathfrak{F}_R}a(\lambda)\Psi^0(\lambda:\bar{n}:h:t)\,d\lambda$$

and $\Phi(a:\bar{n}:h)=\Phi^0(a:\bar{n}:h:0)$.

COROLLARY 2. *There exists an integer* $m\geqq 0$ *with the following property. For any* $a\in C_c^\infty(\omega)$ *and* $h\in A_\mathfrak{p}$, *we can select a positive number* $c(a,h)$ *such that*

$$\|\Phi^0(a:\bar{n}:h:t)\|\leqq c(a,h)(1+t)^m e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for all $\bar{n}\in\bar{N}$ *and* $t\geqq 0$.

We use the notation of [2(i), Lemma 14]. Put $\lambda^*=(-1)^{\frac{1}{2}}\lambda$ and and $e_{\lambda^*}=\sum_{1\leqq i\leqq w}\sigma^i(\lambda^*)u_i$ $(\lambda\in\mathfrak{F}_R)$. Select $v_{kij}\in J$ such that $u_ku_i=\sum_j v_{kij}u_j$ $(1\leqq k,i\leqq w)$ and put $E_{ij}=\sum_k\sigma^k v_{kij}\in S$. Then it is obvious that

$$e_{\lambda^*}u_i\equiv\sum_{1\leqq j\leqq w}E_{ij}(\lambda^*)u_j \bmod SJ_{\lambda^*}\qquad(1\leqq i\leqq w).$$

Let $E(\lambda^*)$ denote the $w\times w$ matrix with the coefficients $E_{ij}(\lambda^*)$. Then we have seen during the proof of Lemma 51 of [2(i)] that[11]

$$E(s\lambda^*)\Xi(\lambda:H_0)=\Xi(\lambda:H_0)E(s\lambda^*)=s\lambda^*(H_0)E(s\lambda^*)\qquad(s\in W)$$

and $\sum_{s\in W}\epsilon(s)E(s\lambda^*)=\pi(\lambda^*)I$ where I is the unit matrix. Hence

$$\pi(\lambda^*)\exp\{-t\Xi(\lambda:H_0)\}=\sum_{s\in W}\epsilon(s)\exp\{-ts\lambda^*(H_0)\}E(s\lambda^*)$$

for $t\in R$ and $\lambda\in\mathfrak{F}_R$. Therefore

$$\Phi^0(a:\bar{n}:h:t)=\sum_{s\in W}\epsilon(s)\int_{\mathfrak{F}_R}a(\lambda)\pi(\lambda^*)^{-1}$$
$$\times\exp\{-ts\lambda^*(H_0)\}E(s\lambda^*)\Phi(\lambda:\bar{n}:h:t)\,d\lambda.$$

But since $E_{ij}\in S$, the statement of the corollary now follows from Lemma 48.

LEMMA 49. *The integral* $\int_{\bar{N}} \| \Phi^0(a:\bar{n}:h:t) \| \, d\bar{n}$ *is convergent for* $a \in C_c^\infty(\omega)$, $h \in A_\mathfrak{p}$ *and* $t \geqq 0$. *Moreover*

$$\int_{\bar{N}} \Phi(a:\bar{n}:h)\, d\bar{n} = \int_{\bar{N}} \Phi^0(a:\bar{n}:h:t)\, d\bar{n} \qquad (t \geqq 0).$$

The first statement is obvious from Corollary 2 of Lemma 48. Moreover it follows from Lemmas 46 and 47 that

$$\Phi^0(a:\bar{n}:h:T) = \Phi(a:\bar{n}:h) + \int_0^T \Psi^0(a:\bar{n}:h:t)\, dt$$

for $T \geqq 0$. On the other hand

$$\Psi^0(a:\bar{n}:h:t) = \sum_{s \in W} \epsilon(s) \int_{\mathfrak{F}_R} a(\lambda)\pi(\lambda^*)^{-1} \times \exp\{-ts\lambda^*(H_0)\} E(s\lambda^*)\Psi(\lambda:\bar{n}:h:t)\, d\lambda.$$

Therefore if we take into account the definition of $\Psi(\lambda:\bar{n}:h:t)$, it follows from Corollary 1 of Lemma 48 that

$$\int \| \Psi^0(a:\bar{n}:h:t \|) \, d\bar{n} \leqq c'(1+t)^m \qquad (t \geqq 0),$$

where c' and m are independent of t. This shows that

$$\int_{\bar{N}} d\bar{n} \int_0^T \| \Psi^0(a:\bar{n}:h:t) \| \, dt < \infty.$$

Hence by Fubini's Theorem,

$$\int_{\bar{N}} \Phi^0(a:\bar{n}:h:T)\, d\bar{n} = \int_{\bar{N}} \Phi(a:\bar{n}:h)\, d\bar{n} + \int_0^T dt \int_{\bar{N}} \Psi^0(a:\bar{n}:h:t)\, d\bar{n}.$$

So in order to prove the second statement of the lemma, it is enough to verify that $\int_{\bar{N}} \Psi^0(a:\bar{n}:h:t)\, d\bar{n} = 0$ for any $t \geqq 0$. But in view of the definition of $\Psi(\lambda:\bar{n}:h:t)$ and the expression for $\Psi^0(a:\bar{n}:h:t)$ in terms of $\Psi(\lambda:\bar{n}:h:t)$ given above, it would be sufficient to show that $\int \phi_a(\bar{n};\eta:h;u)\, d\bar{n} = 0$ for $h \in A_\mathfrak{p}$, $\eta \in \bar{\mathfrak{N}}_1$, $u \in \mathfrak{H}_\mathfrak{p}$ and $a \in C_c^\infty(\omega)$. But this is a consequence of Theorem 3 and Corollary 3 of Lemma 42.

Put $\Phi^0(a:\bar{n}:h:\infty) = \int a(\lambda)\Phi^0(\lambda:\bar{n}:h:\infty)\, d\lambda$ $(a \in C_c^\infty(\omega))$. Then it follows from Lemma 47 that $\Phi^0(a:\bar{n}:h:\infty) = \operatorname*{Lim}_{t \to +\infty} \Phi(a:\bar{n}:h:t)$. On the other hand

$$\int_{\bar{N}} \Phi(a:\bar{n}:h)\,d\bar{n} = \operatorname*{Lim}_{t\to+\infty} \int_{\bar{N}} \Phi^0(a:\bar{n}:h:t)\,d\bar{n}$$

by Lemma 49. From these facts we intend to deduce that

$$\int_{\bar{N}} \Phi_1(a:\bar{n}:h)\,d\bar{n} = \int_{\bar{N}} \Phi_1{}^0(a:\bar{n}:h:\infty)\,d\bar{n}.$$

(Here Φ_1 and $\Phi_1{}^0$ stand for the first coefficients of the one-column matrices Φ and Φ^0 respectively.) However first let us compute $\Phi_1{}^0(\lambda:\bar{n}:h:\infty)$. In order to do this we need the following lemma.

LEMMA 50. *Fix $\bar{n}\in\bar{N}$ and for $h\in A_{\mathfrak{p}}$ let h' denote some element in* $\mathrm{Cl}(A_{\mathfrak{p}}^+)$ *such that $\bar{n}h\in Kh'K$. Then $\|\log h' - \log h - H(\bar{n})\|\to 0$ as* $\min_{\alpha\in P_+}\alpha(\log h)\to+\infty$.

Let σ be an irreducible finite-dimensional representation of G on a vector space V and let Λ denote the highest weight of σ. Select an orthonormal base $\psi_0,\psi_1,\cdots,\psi_p$ for V such that ψ_i belongs to the weight Λ_i $0\leqq i\leqq p$ $(\Lambda_0=\Lambda)$. Put $\|T\| = (\sum_{0\leqq i\leqq p} |T\psi_i|^2)^{\frac{1}{2}}$ for any linear transformation T on V. Then

$$\|\sigma(h')\|^2 = \|\sigma(\bar{n}h)\|^2 = \sum_{0\leqq i\leqq p} |\sigma(\bar{n}h)\psi_i|^2.$$

Let β_i $(1\leqq i\leqq p)$ denote the restriction of $\Lambda-\Lambda_i$ on $\mathfrak{h}_{\mathfrak{p}}$. Then it follows from [2(e), Lemma 2] that $\beta_i\in L_+$ if $\beta_i\neq 0$. Suppose $\beta_i=0$ for $1\leqq i<r$ and $\beta_i\in L_+$ for $r\leqq i\leqq p$. Then the above relation implies that

$$e^{2\Lambda(\log h')}\{r+\sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')}\} = e^{2\Lambda(\log h)}\{\sum_{0\leqq i<r} |\sigma(\bar{n})\psi_i|^2 + \sum_{r\leqq i\leqq p} |\sigma(\bar{n})\psi_i|^2\, e^{-2\beta_i(\log h)}\}.$$

Now suppose $i<r$ and $\alpha\in P_+$. It is obvious that

$$\sigma(H)\sigma(X_\alpha)\psi_i = \{\Lambda(H)+\alpha(H)\}\sigma(X_\alpha)\psi_i$$

for $H\in\mathfrak{h}_{\mathfrak{p}}$. On the other hand α cannot coincide on $\mathfrak{h}_{\mathfrak{p}}$ with $-\beta$ for any $\beta\in L_+$. Therefore $\Lambda+\alpha$ cannot coincide on $\mathfrak{h}_{\mathfrak{p}}$ with Λ_j for any j $(0\leqq j\leqq p)$. This implies that $\sigma(X_\alpha)\psi_i=0$. Hence $\sigma(n)\psi_i=\psi_i$ for $n\in N$ and so $|\sigma(\bar{n})\psi_i| = e^{\Lambda(H(\bar{n}))}$ $(0\leqq i<r)$. Now put $H'(h)=\log h'-\log h-H(\bar{n})$. Then the above equation becomes

$$r+\sum_{r\leqq i\leqq p} |\sigma(\bar{n})\psi_i|^2 \exp\{-2\beta_i(\log h) - 2\Lambda(H(\bar{n}))\} = e^{2\Lambda(H'(h))}\{r+\sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')}\}.$$

Now let $h \to \infty$ in the terminology of Section 9. Then $\beta_i(\log h) \to +\infty$ $(r \leqq i \leqq p)$ and hence we get

$$r = \operatorname*{Lim}_{h\to\infty} e^{2\Lambda(H'(h))} \{r + \sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')}\} \geqq r \operatorname*{Lim\,sup}_{h\to\infty} e^{2\Lambda(H'(h))}.$$

Since $r \geqq 1$, this shows that $\operatorname*{Lim\,sup}_{h\to\infty} \Lambda(H'(h)) \leqq 0$. On the other hand $\bar{n}h = k_1 h' k_2$ $(k_1, k_2 \in K)$ and therefore $H(\bar{n}) + \log h = H(h'k_2)$. But it follows from Lemma 35 of [2(i)] that $\Lambda(\log h') \geqq \Lambda(H(h'k_2))$ and hence $\Lambda(H'(h)) \geqq 0$. This proves that $\operatorname*{Lim}_{h\to\infty} \Lambda(H'(h)) = 0$. This being true for every highest weight Λ, we conclude from Theorem 1 of [2(a)] that

$$\operatorname*{Lim}_{h\to\infty} \| H'(h) \| = 0.$$

Define the function $\boldsymbol{b}_0$ on $\mathfrak{F}_R$ as in Section 9.

LEMMA 51.[11]

$$\Phi_1{}^0(\lambda : \bar{n} : h : \infty) = e^{-\rho(H(\bar{n}))} \sum_{s\in W} \epsilon_0(s) \boldsymbol{b}_0(s\lambda) \exp\{(-1)^{\frac{1}{2}} s\lambda(\log h + H(\bar{n}))\}$$

for $\lambda \in \mathfrak{F}_R$, $\bar{n} \in \bar{N}$ *and* $h \in A_{\mathfrak{p}}$.

Let $\mathfrak{F}_R''$ be the set of all points $\lambda \in \mathfrak{F}_R$ such that $\lambda(s_1 H_0) \neq \lambda(s_2 H_0)$ for any two distinct elements s_1, s_2 in W. Then $\mathfrak{F}_R'' \subset \mathfrak{F}_R'$ and since $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$, it is obvious that $\mathfrak{F}_R''$ is dense in $\mathfrak{F}_R$. Now, for fixed $\bar{n}$ and h, both sides of the above equation are continuous functions of λ (see the corollary of Lemma 47). Therefore it is enough to prove their equality for $\lambda \in \mathfrak{F}_R''$.

Since $\Phi(\lambda : \bar{n} : h : t) = \exp\{t\Xi(\lambda : H_0)\}\Phi^0(\lambda : \bar{n} : h : t)$, it is clear that

$$\pi(\lambda^*)\Phi(\lambda : \bar{n} : h : t) = \sum_{s\in W} \epsilon(s) \exp\{ts\lambda^*(H_0)\} E(s\lambda^*) \Phi^0(\lambda : \bar{n} : h : t)$$

for $t \in R$. (Here the notation is the same as during the proof of Corollary 2 to Lemma 48.) Hence

$$\pi(\lambda^*)\Phi_1(\lambda : \bar{n} : h : t) - \sum_{s\in W} \epsilon(s) \exp\{ts\lambda^*(H_0)\} g_s(\lambda : \bar{n} : h) \to 0$$

as $t \to +\infty$, where

$$g_s(\lambda : \bar{n} : h) = \sum_{1\leqq j\leqq w} E_{1j}(s\lambda^*) \Phi_j{}^0(\lambda : \bar{n} : h : \infty) \qquad (s \in W).$$

On the other hand

$$\Phi_1(\lambda : \bar{n} : h : t) = \pi_0(\lambda) e^{\rho(\log h + tH_0)} \phi_\lambda(\bar{n}h \exp tH_0).$$

Now fix λ, h and $\bar{n}$ $(\lambda \in \mathfrak{F}_R'')$ and for $t \geqq 0$, select an element $h_t' \in \mathrm{Cl}(A_{\mathfrak{p}}{}^+)$ such that $\bar{n}h \exp tH_0 \in Kh_t'K$. Also put $H'(t) = \log h_t' - \log h - tH_0 - H(\bar{n})$.

Then it follows from Lemma 50 that $\| H'(t) \| \to 0$ and therefore $h_t' \to \infty$ (in the termininology of Section 9) as $t \to +\infty$. But

$$e^{\rho(\log h + tH_0)}\phi_\lambda(\tilde{n}h \exp tH_0) = \exp\{-\rho(H(\tilde{n})) - \rho(H'(t))\}e^{\rho(\log h_t')}\phi_\lambda(h_t')$$

and

$$\lim_{h' \to \infty} | e^{\rho(\log h')}\phi_\lambda(h') - \sum_{s \in W} \boldsymbol{c}(s\lambda)\exp\{s\lambda^*(\log h')\}| = 0$$

from Lemma 37 of [2(i)]. Therefore

$$\Phi_1(\lambda : \tilde{n} : h : t) - e^{-\rho(H(\tilde{n}))} \sum_{s \in W} \epsilon_0(s)\boldsymbol{b}_0(s\lambda)\exp\{s\lambda^*(\log h + tH_0 + H(\tilde{n}))\} \to 0$$

as $t \to +\infty$. This implies that

$$\sum_{s \in W} e^{s\lambda^*(tH_0)}\epsilon(s)g_s(\lambda : \tilde{n} : h) - e^{-\rho(H(\tilde{n}))} \sum_{s \in W} \pi(\lambda^*)\epsilon_0(s)\boldsymbol{b}_0(s\lambda)\exp\{s\lambda^*(\log h + tH_0 + H(\tilde{n}))\} \to 0$$

as $t \to +\infty$. But since $\lambda \in \mathfrak{F}_R''$, it follows from Lemma 56 of [2(i)] that

$$g_s(\lambda : \tilde{n} : h) = \pi(\lambda^*)\epsilon(s)\epsilon_0(s)\boldsymbol{b}_0(s\lambda)\, e^{-\rho(H(\tilde{n}))}\exp\{s\lambda^*(\log h + H(\tilde{n}))\} \quad (s \in W).$$

On the other hand $\sum_{s \in W} \epsilon(s)E(s\lambda^*) = \pi(\lambda^*)I$ and therefore

$$\sum_{s \in W} \epsilon(s)g_s(\lambda : \tilde{n} : h) = \pi(\lambda^*)\Phi_1^0(\lambda : \tilde{n} : h : \infty).$$

Hence

$$\pi(\lambda^*)\Phi_1^0(\lambda : \tilde{n} : h : \infty) = \pi(\lambda^*)e^{-\rho(H(\tilde{n}))} \sum_{s \in W} \epsilon_0(s)\boldsymbol{b}_0(s\lambda)\exp\{s\lambda^*(\log h + H(\tilde{n}))\}.$$

The statement of the lemma is now obvious since $\pi(\lambda^*) \neq 0$.

COROLLARY. *The integral* $\int_{\tilde{N}} | \Phi_1^0(a : \tilde{n} : h : \infty)|\, d\tilde{n}$ *converges if* $a \in C_c^\infty(\omega)$ *and* $h \in A_\mathfrak{p}$.

Fix h and a. Then it is obvious that for any $s \in W$,

$$\sup_{H \in \mathfrak{h}_{\mathfrak{p}_0}} (1 + \| H \|)^{k_0} \left| \int_{\mathfrak{F}_R} \boldsymbol{b}_0(s\lambda)a(\lambda)\exp\{s\lambda^*(\log h + H)\}d\lambda \right| < \infty.$$

Hence there exists a positive number c such that

$$| \Phi_1^0(a : \tilde{n} : h : \infty)| \leqq c(1 + \| H(\tilde{n}) \|)^{-k_0}e^{-\rho(H(\tilde{n}))} \qquad (\tilde{n} \in \tilde{N})$$

and from this the corollary follows immediately.

Now we regard the Lie group $\bar{N}$ as an analytic manifold. For any $\nu \in C_c^\infty(\bar{N})$ and $a \in C_c^\infty(\omega)$, put

$$\Phi^0(a:\nu:\bar{n}_0:h:t) = \int_{\bar{N}} \nu(\bar{n})\Phi^0(a:\bar{n}_0\bar{n}:h:t)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}, h \in A_\mathfrak{p}, t \geqq 0)$$

and $\Phi(a:\nu:\bar{n}_0:h) = \Phi^0(a:\nu:\bar{n}_0:h:0)$. It follows from the corollary of Lemma 47 that the integral

$$\Phi^0(a:\nu:\bar{n}_0:h:\infty) = \int_{\bar{N}} \nu(\bar{n})\Phi^0(a:\bar{n}_0\bar{n}:h:\infty)\,d\bar{n}$$

is also well defined.

LEMMA 52. *The integrals*

$$\int_{\bar{N}} \Phi(a:\nu:\bar{n}:h)\,d\bar{n}, \qquad \int_{\bar{N}} \Phi^0(a:\nu:\bar{n}:h:\infty)\,d\bar{n}$$

are both well defined for $a \in C_c^\infty(\omega)$, $\nu \in C_c^\infty(\bar{N})$, $h \in A_\mathfrak{p}$ and they are equal.

In view of Lemma 49 and the right-invariance of the Haar measure of the nilpotent group $\bar{N}$, it is clear that

$$\int \| \Phi(a:\nu:\bar{n}:h) \|\, d\bar{n} \leqq \int |\nu(\bar{n})|\, d\bar{n} \int \| \Phi(a:\bar{n}:h) \|\, d\bar{n} < \infty.$$

Moreover it follows from Lemmas 46 and 47 that

$$\Phi^0(a:\nu:\bar{n}:h:\infty) = \Phi(a:\nu:\bar{n}:h) + \int_0^\infty \Psi^0(a:\nu:\bar{n}:h:t)\,dt$$

where

$$\Psi^0(a:\nu:\bar{n}_0:h:t) = \int \nu(\bar{n})\Psi^0(a:\bar{n}_0\bar{n}:h:t)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}).$$

We claim that

$$\int_{\bar{N}} d\bar{n} \int_0^\infty \| \Psi^0(a:\nu:\bar{n}:h:t) \|\, dt < \infty.$$

If we recall the definition of $\Psi^0(\lambda:\bar{n}:h:t)$ $(\lambda \in \mathfrak{F}_R)$, it becomes clear (see the proof of Lemma 49) that for this it would be sufficient to prove the following lemma. Put $\phi_a(\bar{n}:h) = \phi_a(\bar{n}h)$ $(a \in C_c^\infty(\omega))$ and use the notation of Corollary 1 of Lemma 48.

LEMMA 53. *For any $a \in C_c^\infty(\omega)$ and $\nu \in C_c^\infty(\bar{N})$, put*

$$\phi_a(\nu:\bar{n}_0:h) = \int_{\bar{N}} \nu(\bar{n})\phi_a(\bar{n}_0\bar{n}:h)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}, h \in A_\mathfrak{p}).$$

Then for any $u \in \mathfrak{S}_\mathfrak{p}$ and $h \in A_\mathfrak{p}$, the integral

$$\int_{\bar{N}} d\bar{n} \int_0^\infty |\phi_{a_t}(\nu : \bar{n} ; \eta : h \exp tH_0 ; u)| \times \exp\{\rho(\log h + tH_0) - \beta_0(\log h + tH_0)\} dt$$

is finite.

Let $\xi \to \xi'$ denote the anti-automorphism of $\bar{\mathfrak{N}}$ such that $X' = -X$ $(X \in \bar{\mathfrak{n}})$. Then in view of the left-invariance of the measure $d\bar{n}$, it is clear that

$$\phi_a(\nu : \bar{n} ; \eta : h ; u) = \phi_a(\nu' : \bar{n} : h ; u),$$

where $\nu'(\bar{n}^{-1}) = \nu(\bar{n}^{-1} ; (\eta')^{\bar{n}})$ $(\bar{n} \in \bar{N})$. Hence $\phi_{a_t}(\nu : \bar{n} ; \eta : h \exp tH_0 ; u) = \phi_{a_t}(\nu' : \bar{n} : h \exp tH_0 ; u)$. Now fix ν, h and a. Then from Lemma 48, we can choose a positive constant c and an integer $m \geqq 0$ such that

$$|\phi_{a_t}(\nu' : \bar{n}_0 : h \exp tH_0 ; u)| e^{\rho(\log h + tH_0)} \leqq c(1+t)^m \int |\nu'(\bar{n})| e^{-\rho(H(\bar{n}_0\bar{n}))} \{1 + \rho(H(\bar{n}_0\bar{n}))\}^{-k_0} d\bar{n}$$

for all $\bar{n}_0 \in \bar{N}$ and $t \geqq 0$. Since $\beta_0(H_0) > 0$, the assertion of the lemma is now obvious.

This proves that

$$\int \| \Phi^0(a : \nu : \bar{n} : h : \infty) \| d\bar{n} \leqq \int \| \Phi(a : \nu : \bar{n} : h) \| d\bar{n} + \int d\bar{n} \int_0^\infty \| \Psi^0(a : \nu : \bar{n} : h : t) \| dt < \infty.$$

Therefore it follows by Fubini's Theorem that

$$\int \Phi^0(a : \nu : \bar{n} : h : \infty) d\bar{n} = \int \Phi(a : \nu : \bar{n} : h) d\bar{n} + \int_0^\infty dt \int \Psi^0(a : \nu : \bar{n} : h : t) d\bar{n}.$$

Hence in order to prove Lemma 52, it would be sufficient to verify that

$$\int \Psi^0(a : \nu : \bar{n} : h : t) d\bar{n} = 0$$

for any $t \geqq 0$. But we have seen during the proof of Lemma 49 that the integral $\int \| \Psi^0(a : \bar{n} : h : t) \| d\bar{n}$ is finite and $\int \Psi^0(a : \bar{n} : h : t) d\bar{n} = 0$. Hence it is obvious that

$$\int \Psi^0(a : \nu : \bar{n} : h : t) d\bar{n} = \int \nu(\bar{n}) d\bar{n} \int \Psi^0(a : \bar{n} : h : t) d\bar{n} = 0.$$

This completes the proof of Lemma 52.

Now select ν in such a way that $\int \nu(\bar{n})\,d\bar{n} = 1$. Then it follows from Lemmas 52 and 49 and the corollary of Lemma 51 that

$$\int \Phi_1{}^0(a:\bar{n}:h:\infty)\,d\bar{n} = \int \Phi_1{}^0(a:\nu:\bar{n}:h:\infty)\,d\bar{n}$$
$$= \int \Phi_1(a:\nu:\bar{n}:h)\,d\bar{n} = \int \Phi_1(a:\bar{n}:h)\,d\bar{n}$$

for $a \in C_c^\infty(\omega)$ and $h \in A_\mathfrak{p}$. Now fix a and h and put

$$a_s'(H) = \int \boldsymbol{b}_0(s\lambda)a(\lambda)\exp\{s\lambda^*(\log h + H)\}\,d\lambda$$

for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Then it follows from the theory of Fourier transforms that $\sup_{H \in \mathfrak{h}_{\mathfrak{p}_0}} (1 + \| H \|)^{k_0} |a_s'(H)| < \infty$. On the other hand,

$$\Phi_1{}^0(a:\bar{n}:h:\infty) = e^{-\rho(H(\bar{n}))} \sum_{s \in W} \epsilon_0(s) a_s'(H(\bar{n}))$$

by Lemma 51. Therefore it is obvious that

$$\int \Phi_1{}^0(a:\bar{n}:h:\infty)\,d\bar{n} = \sum_{s \in W} \epsilon_0(s) \int a_s'(H(\bar{n}))\,e^{-\rho(H(\bar{n}))}\,d\bar{n}.$$

Now let δ be a sufficiently small positive number. By the corollary of Lemma 45 of [2(i)], $\int \exp\{-(1+\delta)\rho(H(\bar{n}))\}d\bar{n} < \infty$ and therefore, by Fubini's Theorem,

$$\int a_s'(H(\bar{n}))\exp\{-(1+\delta)\rho(H(\bar{n}))\}d\bar{n}$$
$$= \int \boldsymbol{b}_0(s\lambda)a(\lambda)e^{s\lambda^*(\log h)}\,d\lambda \int \exp\{s\lambda^*(H(\bar{n})) - (1+\delta)\rho(H(\bar{n}))\}d\bar{n}$$
$$= \int \boldsymbol{b}_0(\lambda)a(s^{-1}\lambda)e^{\lambda^*(\log h)}\,\mathrm{conj}\,\boldsymbol{c}(\lambda_\delta)\,d\lambda$$

from Theorem 4 of [2(i)], where $\lambda_\delta = \lambda - (-1)^{\frac{1}{2}}\delta\rho$. But since $\omega \subset \mathfrak{F}_\kappa'$, $\boldsymbol{c}$ is a holomorphic function on a complex neighborhood of ω in $\mathfrak{F}$. Therefore if we recall that ω is invariant under W, it becomes obvious that

$$\int a_s'(H(\bar{n}))\,e^{-\rho(H(\bar{n}))}d\bar{n} = \lim_{\delta \to 0} \int a_s'(H(\bar{n}))\,e^{-(1+\delta)\rho(H(\bar{n}))}d\bar{n}$$
$$= \int \boldsymbol{b}_0(\lambda)a(s^{-1}\lambda)e^{\lambda^*(\log h)}\mathrm{conj}\,\boldsymbol{c}(\lambda)\,d\lambda$$
$$= \int |\boldsymbol{b}_0(\lambda)|^2 \pi_0(\lambda)^{-1}a(s^{-1}\lambda)\,e^{\lambda^*(\log h)}d\lambda.$$

Hence

$$\int \Phi_1^0(a:\tilde{n}:h:\infty)\,d\tilde{n} = \int |\boldsymbol{b}_0(\lambda)|^2 \{\pi_0(\lambda)^{-1} \sum_{s\in W} \epsilon_0(s) a(s\lambda)\} e^{\lambda^*(\log h)} d\lambda.$$

But we have seen above that

$$\int \Phi_1^0(a:\tilde{n}:h:\infty)\,d\tilde{n} = \int \Phi_1(a:\tilde{n}:h)\,d\tilde{n} = e^{\rho(\log h)} \int \phi_a(\tilde{n}h)\,d\tilde{n}.$$

Therefore it follows easily from the corollary of Lemma 43 that $\boldsymbol{\beta}(\lambda) = |\boldsymbol{b}_0(\lambda)|^2$ for $\lambda \in \omega$. But since this holds for any choice of ω and since $\boldsymbol{\beta}$ and $\boldsymbol{b}_0$ are both continuous on $\mathfrak{F}_R$, it is obvious that this relation actually holds for all $\lambda \in \mathfrak{F}_R$.

THEOREM 4. *Let a be an element in $\mathcal{B}(\mathfrak{F}_R)$. Then*

$$e^{\rho(H)} \int_{\bar{N}} \phi_a(\tilde{n} \exp H)\,d\tilde{n} = \int_{\mathfrak{F}_R} |\boldsymbol{b}_0(\lambda)|^2 \{\pi_0(\lambda)^{-1} \sum_{s\in W} \epsilon_0(s) a(s\lambda)\} e^{(-1)^{\frac{1}{2}}\lambda(H)} d\lambda$$

for $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

In view of the result obtained above, this is an immediate consequence of the corollary of Lemma 43, if we use the regular normalization of $d\lambda$. On the other hand the statement of the theorem is obviously independent of the normalization of $d\lambda$. Hence it holds in general.

THEOREM 5. *Let $a \in \mathcal{B}(\mathfrak{F}_R)$ and $\lambda \in \mathfrak{F}_R$. Then*

$$\pi_0(\lambda) \int_G \phi_a(x) \operatorname{conj} \phi_\lambda(x)\,dx = |\boldsymbol{b}_0(\lambda)|^2 \sum_{s\in W} \epsilon_0(s) a(s\lambda)$$

if we use the regular normalizations of dx and $d\lambda$.

This is merely a restatement of the corollary of Lemma 41.

COROLLARY 1. *Let w denote the order of W. Then under the above normalizations,*

$$\int_G |\phi_a(x)|^2\,dx = w^{-1} \int_{\mathfrak{F}_R} |\boldsymbol{b}_0(\lambda)|^2 \,|\sum_{s\in W} \epsilon_0(s) a(s\lambda)|^2\,d\lambda$$

for $a \in \mathcal{B}(\mathfrak{F}_R)$.

This would follow immediately from Theorem 5 by Fubini's Theorem, as soon as we can verify that

$$\int |\pi_0(\lambda)a(\lambda)\phi_\lambda(x)\phi_a(x)|\,dxd\lambda < \infty.$$

This is done as follows. We know (see [2(f), § 12]) that if the Haar measure dh on $A_\mathfrak{p}$ is suitably normalized,

$$\int f(x)\,dx = \int_{A_\mathfrak{p}^+} f(h)\Delta(h)\,dh$$

for any spherical function f in $C_c(G)$. (Here Δ has the same meaning as in Section 13.) Now select an integer $q \geqq 0$ such that

$$c_1 = \int_{A_\mathfrak{p}} (1 + \|\log h\|)^{-q}\,dh < \infty.$$

Then

$$|\pi_0(\lambda)| \int |\phi_\lambda(x)\phi_a(x)|\,dx = |\pi_0(\lambda)| \int_{A_\mathfrak{p}^+} |\phi_\lambda(h)\phi_a(h)|\,\Delta(h)\,dh$$
$$\leqq c_1 \sup_{h \in A_\mathfrak{p}^+} \Delta(h)(1 + \|\log h\|)^q\,|\pi_0(\lambda)\phi_\lambda(h)\phi_a(h)|.$$

Hence it follows from Theorems 1 and 3 that there exists an integer $k \geqq 0$ and, for a fixed a, a positive number c such that

$$|\pi_0(\lambda)| \int |\phi_\lambda(x)\phi_a(x)|\,dx \leqq c(1 + \|\lambda\|)^k$$

for all $\lambda \in \mathfrak{F}_R$. Therefore

$$\int |\pi_0(\lambda)a(\lambda)\phi_\lambda(x)\phi_a(x)|\,dxd\lambda \leqq c \int (1 + \|\lambda\|)^k\,|a(\lambda)|\,d\lambda < \infty.$$

Let $I_0(G)$ denote the subspace of $I(G)$ consisting of all elements of the form ϕ_a $(a \in \mathcal{B}(\mathfrak{F}_R))$.

COROLLARY 2. *For any f in $I(G)$, put*

$$\tilde{f}(\lambda) = \int_G f(x)\,\mathrm{conj}\,\phi_\lambda(x)\,dx \qquad (\lambda \in \mathfrak{F}_R).$$

Then

$$\int_G |f(x)|^2\,dx = w^{-1} \int_{\mathfrak{F}_R} |\boldsymbol{c}(\lambda)|^{-2}\,|\tilde{f}(\lambda)|^2\,d\lambda$$

and

$$f(x) = w^{-1} \int_{\mathfrak{F}_R} |\boldsymbol{c}(\lambda)|^{-2} \tilde{f}(\lambda) \phi_\lambda(x) \, d\lambda$$

for $f \in I_0(G)$ *and* $x \in G$, *if* dx *and* $d\lambda$ *are regularly normalized.*

This is an immediate consequence of Theorems 5 and Corollary 1 above. We have seen (Lemma 29) that $\boldsymbol{c}^{-1}$ is analytic on $\mathfrak{F}_R$. Moreover Theorem 5 of [2(i)] gives a geometric interpretation of $\boldsymbol{c}$.

16. Two conjectures. Let $I_c(G)$ denote the subspace consisting of those elements of $I(G)$ which have compact support. Also let $L_2(G)$ denote the Hilbert space of square-integrable functions on G and $I_2(G)$ the closure of $I_c(G)$ in $L_2(G)$. It is seen without difficulty that $I_c(G) \subset I(G) \subset I_2(G)$. Therefore if the statements of Corollary 2 of Theorem 5 could be extended to all functions $f \in I(G)$, we would immediately get an explicit Plancherel formula (see [2(j)]) for $I_2(G)$. Moreover Theorem 5 of [2(i)] would then provide a simple interpretation for the Plancherel measure. For this, it would obviously be enough to show that $I_c(G) \subset I_0(G)$. However this appears to be a rather difficult problem which I have not yet been able to solve. Its solution seems to depend on the following two unproved statements.

(1) *There exists a polynomial function* $p \in S(\mathfrak{h}_\mathfrak{p})$ *such that* $|\boldsymbol{b}_0(\lambda)p(\lambda)| \geqq 1$ *for all* $\lambda \in \mathfrak{F}_R$.

(2) *For any* $f \in I(G)$, *define* F_f *as in Corollary* 4 *to Lemma* 42. *Then* $F_f \neq 0$ *unless* $f = 0$.

Assuming these two conjectures, we shall show that $I_c(G) \subset I_0(G)$. Let f be any element in $I_c(G)$. Then it follows from Lemma 43 and Corollary 4 of Lemma 42 that $\tilde{f} \in \boldsymbol{\mathcal{B}}(\mathfrak{F}_R)$. On the other hand if we take Lemma 31 into account, it follows from the first conjecture that the function $a(\lambda) = w^{-1}\pi_0(\lambda)|\boldsymbol{b}_0(\lambda)|^{-2}\tilde{f}(\lambda)$ $(\lambda \in \mathfrak{F}_R)$ also lies in $\boldsymbol{\mathcal{B}}(\mathfrak{F}_R)$. Now put $g = \phi_a$. We know from the corollary of Lemma 17 of [2(i)] that $\phi_{s\lambda} = \phi_\lambda (s \in W)$ and therefore $\tilde{f}(s\lambda) = \tilde{f}(\lambda)$ and $\pi_0(\lambda)\tilde{g}(\lambda) = \pi_0(\lambda)\tilde{f}(\lambda)$ $(\lambda \in \mathfrak{F}_R)$ by Theorem 5. Moreover $\tilde{g}$ and $\tilde{f}$ are both continuous functions on $\mathfrak{F}_R$ (see Corollary 3 of Lemma 40). Hence $\tilde{g} = \tilde{f}$. But then by Lemma 43, $F_f = F_g$ and therefore $f = g = \phi_a$ by the second conjecture. This proves that $f \in I_0(G)$ and therefore $I_c(G) \subset I_0(G)$.

Although there seems to be considerable evidence in support of these

conjectures, I have at present no clear idea as to how to proceed to prove them.

COLUMBIA UNIVERSITY.

REFERENCES.

[1] L. Garding, *Math. Scand.*, vol. 1 (1953), pp. 55-72.

[2] Harish-Chandra, (a) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
(b) " " " " vol. 75 (1953), pp. 185-243.
(c) " " " " vol. 76 (1954), pp. 234-253.
(d) " " " " vol. 83 (1956), pp. 98-163.
(e) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(f) " " " vol. 78 (1956), pp. 564-628.
(g) " " " vol. 79 (1957), pp. 87-120.
(h) " " " vol. 79 (1957), pp. 193-257.
(i) " " " vol. 80 (1958), pp. 241-310.
(j) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 40 (1954), pp. 200-204.
(k) " " " " " vol. 43 (1957), pp. 408-409.

[3] F. John, *Proceedings of the Symposium on Spectral Theory and Differential Problems*, Stillwater, Okla., 1951, pp. 113-175.

[4] L. Schwartz, *Théorie des distributions I*, Paris, Hermann, 1950.

ON NILALGEBRAS AND LINEAR VARIETIES OF NILPOTENT MATRICES, I.*

By MURRAY GERSTENHABER.[1]

Let $A_1, \cdots, A_k$ be $n \times n$ matrices with coefficients in a field K having at least n elements, and which have the property that every linear combination of them with coefficients in K is nilpotent. The main purpose of this paper is then to demonstrate that $k \leqq n(n-1)/2$ and if in fact $k = n(n-1)/2$, that there exists a matrix C with coefficients in K such that the CA_iC^{-1} are all triangular matrices. Letting V denote the subspace of n^2-space of all linear combinations of $A_1, \cdots, A_k$, one may say: $\dim V \leqq n(n-1)/2$ and if $\dim V = n(n-1)/2$, then V is in fact an algebra, and one may choose a new basis for the space on which V operates relative to which V is just the algebra of all triangular matrices, where here a triangular matrix shall be one with zeros both below and on the diagonal. For the matrix C of the change of basis one can choose any matrix transforming an arbitrary element of V with nilindex exactly n into triangular form; from what has been asserted, it follows that V indeed contains such an element of maximal nilindex.

The assumption that K has at least n elements is used, as will be seen, to insure that if K' is any extension of K and $V_{K'}$ the linear space obtained by extending the field of definition of V to K', then it is still the case that that every matrix in $V_{K'}$ is nilpotent; one may then say of the variety determined by V that every element in it is nilpotent.

It is easy to exhibit a pair of $n \times n$ matrices with coefficients in a field of fewer than n elements all of whose linear combinations over that field are nilpotent but not over a larger one. Nevertheless, S. A. Hoffman has shown [unpublished] that if three 3×3 matrices with coefficients in the field of two elements have the property that all their linear combinations over that field are nilpotent, then it is still the case that they can simultaneously be brought to triangular form. This suggests that the assumption that K have at least n elements may be unnecessary; no counterexample is yet known to the author.

* Received October 11, 1957; revised January 23, 1958.

[1] The author gratefully wishes to acknowledge the support of the National Science Foundation through contract NSF G-2270 with the University of Pennsylvania.

Proof of the theorem. A necessary and sufficient condition that an $n \times n$ matrix M be nilpotent is that the sum $s_r(M)$ of its $r \times r$ principal minors vanish for all $r = 1, \cdots, n$, for these sums are, up to sign, the coefficients of the characteristic polynomial of M. Let V denote always the given vector space of nilpotent matrices defined over a coefficient field K. If A, B are in V, then $\alpha A + B$ is in V for every α in K, hence is nilpotent, and $s_r(\alpha A + B) = 0$ for $r = 1, \cdots, n$. The expression $s_r(\alpha A + B)$ may be written as a polynomial in α of degree $r - 1$, say

$$s_r(\alpha A + B) = \alpha^{r-1} s_{r,r-1} + \alpha^{r-2} s_{r,r-2} + \cdots + \alpha s_{r,1}, \text{ where } s_{r,i}$$

is simultaneously a homogeneous form of degree i in the coefficients of A and of degree $r - i$ in the coefficients of B. Keeping r fixed and letting α range through the non-zero elements of K, the equations $s_r(\alpha A + B) = 0$ may be viewed as a system of homogeneous linear equations for the $r - 1$ unknowns $s_{r,i}$. Since $r \leqq n$, there are, by assumption, at least $r - 1$ distinct non-zero elements of K. Choosing such a set of elements, the determinant of the system is of Vandermonde type and does not vanish; therefore $s_{r,i} = 0$ for all r and i. It follows that $s_r(xA + B) = 0$ for x in any extension K' of K, whence $xA + B$ is nilpotent. Equivalently, $x_1 A_1 + x_2 A_2$ is nilpotent, where x_1, x_2 are arbitrary elements of K' and A_1, A_2 are arbitrary elements of V. Now if it has been shown that any linear combination of, say, t elements of V with coefficients in K' is nilpotent, then it follows that

$$x_1 A_1 + \cdots + x_{t-1} A_{t-1} + x_t (A_t + \alpha A_{t+1})$$

is nilpotent for all $x_1, \cdots, x_t$ in K', $A_1, \cdots, A_{t+1}$ in V, and α in K. By the same argument as that just given, it follows that one may again replace α by an element of K', whence $x_1 A_1 + \cdots + x_t A_t + x_{t+1} A_{t+1}$ is also nilpotent for all $x_1, \cdots, x_{t+1}$ in K', and by induction, this holds for all t. We may, therefore, whenever it is suitable, enlarge the field of definition for V, and it will remain the case that every matrix in the enlarged linear space is nilpotent. Therefore, in general, no subscript will be used to indicate the field of definition, particularly when it is clear from the context.

If the linear variety V is spanned by $A_1, \cdots, A_k$, then a generic element of V over K is a matrix of the form $x_1 A_1 + \cdots + x_k A_k$, where $(x) = (x_1, \cdots, x_k)$ is a set of k independent transcendentals over K. The elements of this generic matrix are linear functions l_{ij} of $x_1, \cdots, x_k$ and may be viewed as vectors in a k-dimensional space with components $((A_1)_{ij}, \cdots, (A_k)_{ij})$. This set of vectors indexed by pairs of indices (i, j), $i, j = 1, \cdots, n$ may be considered associated with the variety V and uniquely

determines it. For convenience, we shall occasionally denote a pair of indices (i, j) by a single symbol, say σ, and the corresponding vector by l_σ. Among the vectors l_σ the number of linearly independent ones is dim V.

If X is any $n \times n$ matrix with coefficients in an extension field of K and with non-vanishing determinant, then we may form the linear variety $V(X) = XVX^{-1}$ defined over the field $K(X) = K((x_{ij}))$; it has the same dimension as V, and every matrix in it is again nilpotent. The vectors associated with $V(X)$ will be denoted by $l_{ij}(X)$ or $l_\sigma(X)$; for $X = 1$, we will write as before just l_σ. If S is a subset of the set of all pairs of indices (i, j), $i, j = 1, \cdots, n$, then the linear space spanned by the $l_\sigma(X)$, $\sigma \in S$, will be denoted by $L_S(X)$. If S and S' are two sets of pairs of indices such that $L_{S'}(X) \subseteq L_S(X)$, then S' will be said to be dependent on S; such dependencies usually vary with X. Further, if $\dim L_S(X) = \dim V$, then every S' is dependent on S and S will be called complete.

Given τ, S, and X such that $l_\tau(X) \in L_S(X)$, then we may write $l_\tau(X) = \sum a_\sigma(X) l_\sigma(X)$, the summation ranging over $\sigma \in S$, where $a_\sigma(X)$ is an element of $K(X)$. If Y is a specialization of X over K with non-zero determinant, it does not necessarily follow that $l_\tau(Y) \in L_S(Y)$; for some $a_\sigma(Y)$ may not be finite, although, since there always exists a σ_0 for which all $a_\sigma(Y)/a_{\sigma_0}(Y)$ are finite [1], one finds, in that case, a dependence relation between the $l_\sigma(Y)$ for $\sigma \in S$. However, if Y is a generic specialization of X, then certainly all $a_\sigma(Y)$ are finite and we may write $l_\tau(Y) = \sum a_\sigma(Y) l_\sigma(Y)$.

The set of all pairs of indices (i, j), $i, j = 1, \cdots, n$, may be divided naturally into three disjoint subsets: δ_+, the set of all (i, j) with $j > i$, i.e., the elements above the diagonial; δ_0, the set of all (i, j) on the diagonal; and δ_-,the set of all (i, j) with $j < i$, or the elements below the diagonal. Given a $\sigma = (i, j)$, we may occsionally write σ^* for the pair (j, i). The set of all σ^* for σ in a set S will then be denoted by S^*. Instead of L_{δ_+}, we will write simply L_+; analogous definitions will hold for L_0 and L_-.

For a linear variety of nilpotent matrices, it is always the case that δ_0 is dependent on δ_+ (and, of course, δ_-), else there would exist a matrix in V with zero entries above the diagnoal and a non-zero entry somewhere on the diagonal; but such a matrix can not be nilpotent. Since $V(X) = XVX^{-1}$ is also a linear variety of nilpotent matrices, the same holds for it. From this will follow now the first major lemma in the proof of our proposition: Let X be a matrix whose elements are n^2 independent transcendental quantities over K, the field of definition for V. Then $L_+(X)$ is complete.

Since $L_0(X) \subseteq L_+(X)$, were this false there would exist a $\tau = (i, j)$

in δ_- such that $l_\tau(X) \notin L_+(X)$; assume τ so chosen that $i-j$ is minimal. To see that this leads to a contradiction, we shall consider the effect of replacing X by $X' = (1 + ze_{\tau^*})X$, where z is transcendental over $K(X)$ and e_{τ^*} is the matrix with 1 in the j-th row, i-th column, and zeros elsewhere. Given a matrix A, the matrix $(1 + ze_{\tau^*})A(1 + ze_{\tau^*})^{-1}$ is obtained from A by adding z times the i-th row to the j-th and then subtracting z times the j-th column from the i-th (for note that $(1 + ze_{\tau^*})^{-1} = 1 - ze_{\tau^*}$). Let now S denote $\delta_+ - \tau^*$. Then it is the case that $L_S(X') \subseteq L_S(X)$. For if $\sigma \in \delta_+$ but σ not in the j-th row or i-th column, then $l_\sigma(X') = l_\sigma(X)$. If $\sigma \in \delta_+$ and σ in the j-th row but $\sigma \neq \tau^*$, then we may set $\sigma = (j, k)$ and $l_{jk}(X') = l_{jk}(X) + zl_{ik}(X)$. Here $k > j$, and by choice of τ, for such k, we have $l_{ik}(X) \in L_+(X)$ (for note that this is so for $k > j$ but $k < i$ by choice of τ; that $l_{ii}(X) \in L_+(X)$ since δ_0 is dependent on δ_+; and that $l_{ik}(X) \in L_+(X)$ by definition for $k > i$). Therefore, $l_{jk}(X')$, being a linear combination of elements of $L_+(X)$, is in $L_+(X)$, where, however, we must now construe $L_+(X)$ as a vector space over $K(X, z)$. Similarly, for $\sigma \in \delta_+$, σ in the i-th column but $\sigma \neq \tau^*$, we have $\sigma = (k, i)$ and $l_{ki}(X') = l_{ki}(X) - zl_{kj}(X)$. Therefore, for all $\sigma \in S$, we have $l_\sigma(X') \in L_S(X)$, so $L_S(X') \subseteq L_S(X)$. However, for $l_{\tau^*}(X')$, we have $l_{\tau^*}(X') = l_{\tau^*}(X) + zl_{ii}(X) - zl_{jj}(X) - z^2 l_\tau(X)$, and for $l_{jj}(X')$, we have $l_{jj}(X') = l_{jj}(X) + xl_\tau(X)$. Now $l_{jj}(X')$ is in $L_+(X')$, and from these equations and the fact that $l_{\tau^*}(X)$ and $l_{jj}(X)$ are in $L_+(X)$ but $l_\tau(X)$ is not, it follows that $l_{jj}(X') = -z^{-1}l_{\tau^*}(X') + \sum a_\sigma(X')l_\sigma(X')$, where the sumation ranges over σ in S. Therefore,

$$zl_{jj}(X') = -l_{\tau^*}(X') + z\sum a_\sigma(X')l_\sigma(X'),$$

and this is an identity in z, where X' may be considered a function of z taking on the value X when $z = 0$. Since the entries in X are independent transcendentals over K, it is the case that any matrix X' is a specialization of X over K, but since z is transcendental over $K(X)$, it follows that the entries in X' are likewise independent transcendentals over K; so X and X' are generic specializations of each other. Therefore $a_\sigma(X)$ is finite for all $\sigma \in S$, and setting $z = 0$, we find $l_{\tau^*}(X) = 0$. But again, since X' is a generic specialization of X, it follows that $l_{\tau^*}(X') = 0$, and from the equation for $l_{\tau^*}(X')$, we find $0 = zl_{ii}(X) - zl_{jj}(X) - z^2 l_\tau(X)$ which implies that $l_\tau(X) \in L_0(X) \subseteq L_+(X)$, contrary to assumption. Therefore, indeed, if the elements of X are n^2 independent transcendental quantities over K, then $L_+(X)$ is complete.

Since δ_+ contains only $n(n-1)/2$ elements, it follows that $\dim V \leq n(n-1)/2$, which proves the first half of our main proposition. We shall

suppose henceforth that $\dim V = n(n-1)/2$, and we must show that V is then similar to the set of all triangular matrices. Since by choosing X a generic $n \times n$ matrix over the field K of definition for V, we have $L_+(X)$ complete, we shall henceforth assume simply that the transformation has been made and L_+ is complete. We must assume, however, that the field of definition, K, has been extended to $K(X)$, a pure transcendental extension of dimension n^2 over K.

Let P now be any invertible $n \times n$ matrix with zeroes above the diagonal and remaining coefficients in $K(X)$. We may form $V(P) = PVP^{-1}$ and $L_+(P)$. It is then the case that $L_+(P) = L_+$. For if A is any matrix in V and P, as before, has zeros above the diagonal, then the i-th row of PA is a linear combination only of rows $1, \cdots, i$ of A. Similarly, if Q has zeros above the diagonal, then the j-th column of AQ is a linear combination of columns $1, \cdots, j$, and P^{-1} is such a Q. Therefore, if $\sigma \in \delta_+$, then $l_\sigma(P)$ is a linear combination of l_σ's for $\sigma \in \delta_+$, so $L_+(P) \subseteq L_+$. Transforming by P^{-1}, the reverse inclusion holds, so indeed $L_+(P) = L_+$.

Suppose now that $\dim V = n(n-1)/2$ and that L_+ be complete. Since δ_+ has only $n(n-1)/2$ elements, there must exist a matrix $A = (a_{ij})$ in V for which $a_{i,i+1} = 1$, $i = 1, \cdots, n-1$, and $a_{ij} = 0$ for $j > i+1$. Of the entries in A below the diagonal nothing need be known, but it is the case, nevertheless, that A, being nilpotent, has index exactly n. For letting $e_1, \cdots, e_n$ now denote the basis of the space on which the elements of V operate, the i-th row of A is just e_iA. But then from the form of A, we have $e_1A = e_2 +$ multiple of e_1, $e_1A^2 = e_3 +$ linear combination of e_1 and e_2, etc., so that $e_1A^{n-1} = e_n +$ linear combination of e_1 to e_{n-1}; hence A^{n-1} is not zero. Therefore, if $\dim V = n(n-1)/2$, it must contain at least one element of index exactly n.

Let $N = (\nu_{ij})$ denote the matrix for which $\nu_{i,i+1} = 1$, $i = 1, \cdots, n-1$, $\nu_{ij} = 0$ for $j \neq i+1$. Then N is nilpotent of index n and is the Jordan canonical form for any $n \times n$ matrix of index n. Although usually a matrix can be transformed into Jordan canonical form only over an algebraically closed field, if A is any matrix of index n, then there exists a matrix P such that $PAP^{-1} = N$ and the elements of P are in the field of definition for A. In fact, for P, we may choose the matrix whose rows are $e_1, e_1A, \cdots, e_1A^{n-1}$, for relative to these vectors as basis, the linear transformation A has the matrix N. For the matrix A given above ($a_{i,i+1} = 1$, $i = 1, \cdots, n-1$, $a_{ij} = 0$ for $j > i+1$), the matrix P whose rows are $e_1, e_1A, \cdots, e_1A^{n-1}$ has zeros above the diagonal since the i-th row of P is $e_1A^{i-1} = e_i +$ linear combination of e_1 to e_{i-1}. Therefore $L_+(P) = L_+$, whence $L_+(P)$ is still complete, and

further, $V(P) = PVP^{-1}$ contains the matrix N. We may therefore assume henceforth that L_+ is complete and that V contains N. It is then already the case, as we shall see, that V is the algebra of all $n \times n$ triangular matrices. To show this, we shall have to prove that V contains not only N but also $N^2, N^3, \cdots, N^{n-1}$.

Denoting, as before, by $s_r(M)$ the sum of the $r \times r$ principal minors of M and setting $s_r(\alpha A + B) = \alpha^{r-1}s_{r,r-1} + \cdots + \alpha s_{r,1}$, we have observed that s_{ri} is a doubly homogeneous form of degree i in the coefficients of A and of degree $r - i$ in those of B and that s_{ri} vanishes for all A and B in V. Let us set $A = (a_\sigma)$, and if σ is the pair (i, j), then σ^* will denote, as before, (j, i). Then s_{21} is a bilinear form in the elements of A and B, and a simple computation shows that $s_{21} = \sum a_{\sigma^*} b_\sigma$, the summation ranging over all pairs of indices σ. Keeping A fixed and varying B, we see that if A is in V, then a dependence relation between the vectors l_σ of the form $\sum a_{\sigma^*} l_\sigma = 0$ must hold. Let us now denote by D the set of all triangular matrices in V and by D' the set of all triangular matrices $A = (a_\sigma)$ for which $\sum a_{\sigma^*} l_\sigma = 0$ holds. Then D and D' are linear spaces, and it follows from what has just been shown that $D \subseteq D'$. If A is triangular, then $\sum a_{\sigma^*} l_\sigma = 0$ is a relation involving only those l_σ for σ in δ_-, i. e., below the diagonal, and it is clear then from the definition of D' that $\dim L_- = n(n-1)/2 - \dim D'$. But L_+ is complete and has dimension $n(n-1)/2$; therefore $\dim D = n(n-1)/2 - \dim L_+$ (for a matrix in V with zeros below the diagonal is in fact triangular). We see therefore that $\dim D = \dim D'$, whence in fact $D = D'$. Since it has been shown that V contains N, we may choose N for B, and with that choice, the s_{r1}, being linear forms in the elements of A, are easily computed. In fact, $s_{r1} = \sum a_{i+r-1,i}$, the sum ranging from $i = 1$ to $i = n - r + 1$. Since $s_{r1} = 0$ for all A in V, it is therefore the case that $\sum l_{i+r-1,i} = 0$ for $r = 1, \cdots, n$. Now for $r = 2, \cdots, n$, the pairs $(i + r - 1, i)$ are all in δ_-, and the relation $\sum l_{i+r-1,i} = 0$ is in fact equivalent to having N^{r-1} in D'. Therefore N^{r-1} is in D for $r = 2, \cdots, n$, which implies that V contains not only N but $N^2, N^3, \cdots, N^{n-1}$ as well. It follows, therefore, that if a matrix A is in V, then $A + \alpha_1 N + \cdots + \alpha_{n-1} N^{n-1}$ is nilpotent for all $\alpha_1, \cdots, \alpha_{n-1}$. But we shall show that this implies that A is actually triangular.

Suppose now that $A = (a_{ij})$ has the property that $A + \alpha_1 N + \cdots + \alpha_{n-1} N^{n-1}$ is nilpotent for all $\alpha_1, \cdots, \alpha_{n-1}$. Choosing $\alpha_i = -a_{1,j+1}$, the first row of the matrix $A + \alpha_1 N + \cdots, \alpha_{n-1} N^{n-1}$ is $(a_{11}, 0, \cdots, 0)$. Therefore, $a_{11} = 0$, else $A + \alpha_1 N + \cdots + \alpha_{n-1} N^{n-1}$ would have a non-zero latent root. Let P now be the matrix $1 + \beta_1 N + \cdots + \beta_{n-1} N^{n-1}$. Then P is non-singular and commutes with N, whence $A + \alpha_1 N + \cdots + \alpha_{n-1} N^{n-1}$ is nilpotent for all

$\alpha_1, \cdots, \alpha_{n-1}$ if and only if $PAP^{-1} + \alpha_1 N + \cdots + \alpha_{n-1}N^{n-1}$ has the same property. Therefore, for every choice of $\beta_1, \cdots, \beta_{n-1}$, the element in the first row and column of PAP^{-1} must be zero. It follows that the first column of A is zero, for choosing $\beta_i = 1$ and $\beta_j = 0$ for $j \neq i$, the element in the first row and column of PAP^{-1} is $a_{i+1,1}$. Let $e_1, \cdots, e_n$ be, as before, the basis vectors for the space $\bar{E}$ on which the matrices of V (defined now over $K(X)$) operate and let $\bar{E}'$ denote the subspace of $\bar{E}$ spanned by $e_2, \cdots, e_n$. Then it is clearly the case that $\bar{E}N$ is contained in $\bar{E}'$, and we have just shown, in effect, that $\bar{E}A$ is contained in $\bar{E}'$ also. In particular, $\bar{E}'$ is carried into itself by both N and A, and we may consider, therefore, the restrictions of N and A to this space; the matrices of these restrictions are obtained by striking out the first row and column from the matrices of N and A, respectively. Now for $n = 1$, the lemma in question is trivial, and we may therefore make the inductive assumption that it holds for all smaller values of n than the one we are considering. Stripped of its first row and column, therefore, the matrix of A is triangular; but since the first column is zero, A itself is triangular, which was to be proved.

It has therefore been shown that if V is a linear space of nilpotent $n \times n$ matrices wtih elements in a field K having at least n elements, and if $\dim V = n(n-1)/2$, then there exists a matrix which we will denote by Y such that every matrix in YVY^{-1} is triangular. If K is the field of definition for V, then Y may be taken to have coefficients in a field $K(X)$, where $X = (x_{ij})$ is a set of n^2 independent transcendental quantities over K. It was asserted, however, that one could choose for Y a matrix C with coefficients in K, and this must still be shown. Let E now denote the n-dimensional vector space over K on which the matrices of V, defined over K, operate. We must prove, in effect, that a basis can be chosen for E relative to which every matrix of V is triangular. Agreeing with the previous notation, $\bar{E}$ will denote the space obtained by extending the field of coefficients to $K(X)$. Then we have seen that $V_{K(X)}$ is similar, over $K(X)$, to the algebra of all triangular matrices. It follows, therefore, that there exists a non-zero vector in $\bar{E}$ which is annihiliated by every matrix in $V_{K(X)}$, or what is the same thing, that the intersection of the null spaces of the elements of $V_{K(X)}$ is of positive dimension. From this, it follows that the intersection of the null spaces of the elements of V (these are subspaces of E) is not zero, being in fact of the same dimension. There exists, then, a non-zero vector v in E annihiliated by every matrix of V. Let (v) denote the linear space spanned by v and E^* the quotient space $E/(v)$. Then every element A of V induces a linear transformation of E^* whose matrix is that obtained from A by

deleting the last row and column. Of the $2n-1$ elements deleted from A, n are zero; hence if V^* denotes the linear space of operators on E^* so obtained, $\dim V^* \geqq n(n-)/2-(n-1)=(n-1)(n-2)/2$. Now the theorem is trivial for $n=1$, and we have $\dim E^*=n-1$. We may therefore make the inductive assumption that a basis $v_1^*,\cdots,v_{n-1}^*$ can be chosen for E^* relative to which every matrix in V^* is triangular. Then letting $v_1,\cdots,v_{n-1}$ be representatives for $v_1^*,\cdots,v_{n-1}$, v form a basis of E relative to which every matrix of V is triangular.

From the foregoing, one sees that there indeed exists a matrix C with coefficients in K such that CVC^{-1} is the algebra of all triangular matrices. It was asserted, lastly, that if A is any element of V of index exactly n, then it is sufficient to choose for C any matrix Q such that QAQ^{-1} is triangular. One may show by direct computation that if M is a triangular matrix of index n and P a non-singular matrix such that PMP^{-1} is again triangular, then P has zeros below the diagonal. Therefore, if A has index n and if Q is a matrix such that QAQ^{-1} is triangular, then Q is unique up to left multiplication by such a matrix P with zeros below the diagonal. Thus if C is a matrix such that CVC^{-1} is the algebra of all triangular matrices, then, in particular, CAC^{-1} is triangular, so $C=PQ$ for some P with zeros below the diagonal. Then $CVC^{-1}=P(QVQ^{-1})P^{-1}$, but conjugation by P carries the set of all triangular matrices onto itself, so that it must already be the case that every matrix in QVQ^{-1} is triangular. In order to effect the actual reduction of V to the set of triangular matrices, the only problem that remains is the finding of an element of index n. If $A_1,\cdots,A_k$, $k=n(n-1)/2$, is a basis for V and $x_1,\cdots,x_k$ are independent transcendentals over K, then $A(x_1,\cdots,x_k)=x_1A_1+\cdots+x_kA_k$, being a generic point of V over K, has index n, but has coefficients in $K(X)$. There must exist a specialization of $x_1,\cdots,x_k$ in K for which $A^{n-1}\neq 0$; it is therefore a finite process to find such a specialization, and this, in principle, solves the problem. Somewhat easier, perhaps, is to find a Y with coefficients in the ring $K[X]$ such that $YA(x_1,\cdots,x_n)Y^{-1}=N$. We know that there must exist a specialization of $(x_1,\cdots,x_n)$ in K over which Y and Y^{-1} have finite specializations C and C^{-1}; this gives the desired C.

Comments. The orginial motivation for the present paper is in the following theorem whose proof will be given in the second paper of this series: Let $\mathfrak{A}$ be a commutative, not necessarily associative and not necessarily finite dimensional algebra over a field of characteristic zero, and suppose there exists an integer t such that the t-th power of every element of $\mathfrak{A}$ in every association vanishes. Then the linear transformation $R_a: x\to xa$ of $\mathfrak{A}$ onto

itself is nilpotent for every a in $\mathfrak{A}$ (in fact of index not more than $2t-3$). If $\mathfrak{A}$ is finite dimensional, then the set of right multiplications R_a, for all a in $\mathfrak{A}$, is precisely a linear space of nilpotent matrices. Unfortunately, the theorem proved here yields only meager results about such non-associative nilalgebras. A more complete description of linear varieties of nilpotent matrices would probably shed further light even on the structure of the radical of an associative algebra. It is interesting to note that there is nothing in the statement of the main theorem of this paper that involves an extension of the the field of definition. Nevertheless, transcendental extensions, or what are in effect algebrized versions of geometric arguments, played an important role in the proof. Such arguments may be unnecessary, but it is also possible that they may prove a valuable tool in studying the structure of the radical of an algebra.

Finally, the author wishes to thank Professor Olga Taussky-Todd for ideas communicated in personal correspondence, and Professor A. A. Albert for much help and stimulation.

INSTITUTE FOR ADVANCED STUDY,
UNIVERSITY OF PENNSYLVANIA.

REFERENCE.

[1] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, New York, 1946. (Chapter II, Proposition 10.)

ON THE STRUCTURE OF LOCAL HOMEOMORPHISMS OF EUCLIDEAN n-SPACE, II.*

By SHLOMO STERNBERG.

1. In this paper we continue the study of local homeomorphisms of n-space begun in [6]. The main result is that every C^∞ mapping of some neighborhood of the origin onto itself, keeping the origin fixed, is equivalent via a C^∞ change of coordinates to a linear transformation, provided that a certain formal condition on the Jacobian is satisfied. If this condition is violated but no eigenvalue is of absolute value one, we show that the transformation can be brought to a simple but non-linear normal form. This result was proved in [6] for the case of contractions; the remaining cases will be treated here. In view of the connection between local mappings and differential equations (cf. Lemma 4 of [6]), our results include a C^∞ version of a well known theorem of Siegel [3] and results of Birkhoff [1] and Birkhoff and Bamforth [2]. The theorem becomes false when extended to the analytic case. In future publications we shall deal with the analytic case, and study in some detail the structure and representations of various groups of local mappings. We shall also see the true meaning of conditions (*) below in terms of the root structure of the group of all local maps.

In Section 2 we state the theorem and give a sketch of the proof in two dimensions. In Sections 3 and 4 we prove some preparatory lemmas and in Section 5 we complete the proof of the main theorem. Sections 6 and 7 are devoted to a discussion of applications and of the situation where condition (*), below, is violated.

We should like to thank Dr. Fred Brauer for many helpful conversations. Above all, we wish to thank Professor Wintner for his encouragement and advice throughout the progress of this work.

2. We now state the main theorem.

THEOREM 1. *Let T be a homeomorphism of class C^1 of $E^n \to E^n$ defined in some neighborhood of the origin, keeping the origin fixed. Let $s_1, \cdots, s_n$ be the (possibly complex or multiple) eigenvalues of $J(T)$, where $J(T)$ is the Jacobian of T at the origin. Then if*

* Received December 30, 1957.

(*) *$s_i \neq s_1^{m_1} \cdots s_n^{m_n}$ for all non-negative integers $m_1, \cdots, m_n$ with $\sum m_i > 1$ holds, there exist a neighborhood N of the origin and a function $\lambda = \lambda(s_1, \cdots, s_n; l)$ such that there is a change of coordinates R of class λ defined in N which linearizes T. Furthermore, for any fixed $s_1, \cdots, s_n$, $\lambda(s_1, \cdots, s_n; l) \to \infty$ as $l \to \infty$. In particular, for $l = \infty$, R can be chosen to be of class C^∞.*

We first observe that (*) implies that $|s_i| \neq 0, 1$ for any i. The first inequality is trivial and the second follows from the fact that since $J(T)$ is real, any eigenvalue occurs along with its complex conjugate. If we set $r_i = |s_i|^2$, we can order the r_i as

$$0 < r_1 < \cdots < r_k < 1 < r_{k+1} < \cdots < r_n. \tag{1}$$

For the purposes of this paper, we may assume that $0 < k < n$. In fact, if $k = n$, the mapping T is a contraction, and if $k = 0$, T^{-1} is. Both of these cases have been treated in [6]. We shall now sketch a proof of Theorem 1 for the case $n = 2$, $l = \infty$, in orded to motivate the considerations of the following sections. By Theorem 7 of [6] or Theorem 5 of [4], we can assume that the axes are invariant curves. Furthermore, (*) implies that a formal change of coordinates can be found which formally linearizes T. Choosing coordinates properly, we can then assume that T has the form

$$x_1 = sx[1 + f(x, y)], \qquad y_1 = ty[1 + g(x, y)], \tag{i}$$

where we can assume that

$$0 < s < 1 < t \tag{ii}$$

and

$$f(x, y) = o((x^2 + y^2)^m) \text{ and } g(x, y) = o((x^2 + y^2)^m) \text{ for all } m. \tag{iii}$$

We can also assume, by [5] or [6] Theorem 2, that $f(x, 0) = g(0, y) = 0$. We then seek a change of coordinates

$$\bar{x} = x\phi(x, y), \qquad \bar{y} = y\psi(x, y) \tag{iv}$$

which linearizes (i). Since the four quadrants are left invariant by (i), it suffices to construct ϕ and ψ in each of them and to prove that ϕ and ψ tend to 1, together with all their derivatives, as a point approaches the axis. The functional equation to be satisfied by ϕ, for example, is $sx[1 + f(x, y)]\phi(x_1, y_1) = sx\phi(x, y)$ or

$$\phi(x_1, y_1) = [1 + f(x, y)]^{-1}\phi(x, y). \tag{v}$$

Now we can view (v) as defining ϕ at (x_1, y_1) when $\phi(x, y)$ is known. If we choose ϕ to be identically one on the line $C: y = x$, then (v) defines ϕ on

the images C^n of C. If (i) were actually linear, these images would be the lines $t^{-n}y = s^{-n}x$, which tend to the axes as $n \to \pm\infty$. Since (i) doesn't differ very much from its linear part, the images C^n also approach the axes as $n \to \pm\infty$. In the case of (i) which is defined only in some small neighborhood of the origin, any point will eventually get out of N. What we mean by C^n approaching an axis is that $C^n \cap N$ does. If we call W the region bounded by C^1 and C^1 and contained in N, we can define ϕ in W so as to be C^∞ and to be $=1$ on C and to satisfy (v) which imposes a condition only on C^1. We then define ϕ on $W^n \cap N$ as

$$\phi(x_n, y_n) = [1 + f(x, y)]^n \phi(x, y). \tag{vi}$$

The point now is that, although n may become arbitrarily large, in order for all the images (x_k, y_k) of (x, y) to remain in N for $k \leqq n$ and n large, (x, y) must be very close to the origin; this makes $f(x, y)$ small enough to prevent any difficulty.

In the general case, no simple pre-normal form such as (i) exists and, since complex eigenvalues can enter, no '2^n-tant' need be left invariant. We can carry out the proof by replacing the half line $x = y > 0$ by the complete cone $x^2 = y^2$ or, in general, a similar cone in n dimensions.

3. In this section, we study in some detail the linear transformation L without multiple elementary divisors whose eigenvalues, s_i, satisfy (*). We first choose coordinates x_i corresponding to these eigenvalues. We then introduce the following three norms

$$\| x \|_+ = x_1^2 + \cdots + x_k^2, \qquad \| x \|_- = x_{k+1}^2 + \cdots + x_n^2,$$
$$\| x \| = \| x \|_+ + \| x \|_- = x_1^2 + \cdots + x_n^2,$$

where k is given by (1). We also introduce the cone

$$C: x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_n^2 = 0.$$

On C, $\| x \|_+ = \| x \|_- = \frac{1}{2} \| x \|$ and the complement of C consists of two open sets

$$S_+ = \{x \mid \| x \|_+ < \| x \|_-\}$$

and

$$S_- = \{x \mid \| x \|_- < \| x \|_+\}.$$

It is clear that $LS_+ \subset S_+$; in fact, any point of LS_+ satisfies $\| x \|_+ / \| x \|_- \leqq r_k / r_{k+1}$. Similarly, $\bigcap_{n=0}^{\infty} L^n S_+ = I_+$, where I_+ is the subspace $I_+ = \{x \mid \| x \|_+$

$=0\}$. Let W denote the closed wedge $W = \overline{(S_+ - LS_+)}$; W is bounded by C and the cone

$$C_1 : r_1^{-1}x_1^2 + \cdots + r_k^{-1}x_k^2 - r_{k+1}^{-1}x_{k+1}^2 - \cdots r_n^{-1}x_n^2 = 0.$$

We collect these facts as

LEMMA 1. *The closure of the set S_+ can be decomposed into the union*

$$\bar{S}_+ = \left(\bigcup_{n=0}^{\infty} L^n W\right) \cup I_+. \tag{2}$$

For any $y \in L^m W$, we have the inequality

$$r_1^{m+1}/r_k^{m+1} \leqq \| y \|_+ / \| y \|_- \leqq r_k^m / r_{k+1}^m. \tag{3}$$

Now for any point x in the space,

$$r_1^m \| x \|_+ \leqq \| L^m x \|_+ \leqq r_k^m \| x \|_+ \tag{4}$$

and

$$r_{k+1}^m \| x \|_- \leqq \| L^m x \|_- \leqq r_n^m \| x \|_-. \tag{5}$$

If $x \in W$, then a consequence of (3) for $m = 0$ is

$$2 \| x \|_+ \leqq \| x \| \leqq (r_1 + r_n)/r_1 \| x \|_+ \tag{6}$$

and

$$(r_1 + r_n)/r_n \cdot \| x \|_- \leqq \| x \| \leqq 2 \| x \|_-. \tag{7}$$

If we combine (5) with (7) we obtain, for $x \in W$

$$\| L^m x \| \geqq \| L^m x \|_- \geqq \tfrac{1}{2} r_{k+1}^m \| x \|. \tag{8}$$

In particular, we have

LEMMA 2. *Let B_r denote the ball of radius r and let $W_r = W \cap B_r$. Then*

$$B_{\frac{1}{2}r}^+ = B_{\frac{1}{2}r} \cap S_+ \subset \bigcup_{n=0}^{\infty} (L^m W_r) \cup (I_+ \cap B_r). \tag{9}$$

If we set $W_r^m = L^m W \cap B_r$, then another consequence of (8) is that the set $L^{-m} W_r^m$ is very small for large m. More explicitly, we have

LEMMA 3. *Let D_r^m denote the set $2r_{k+1}^{-m} W_r$, then*

$$L^{-m} W_r^m \subset D_r^m. \tag{10}$$

In particular, if $x \in L^{-m-1} W_r^{m+1}$, then x can be written in the form

$$x = r_{k+1}^{-1} x^*, \qquad x^* \in D_r^m. \tag{11}$$

Finally, if $y \in B_1^+ - I_+$, then $y = L^m x$ for some $x \in W$. We shall call x a pre-image of y. Combining (4), (6) and (8), we obtain an estimate of $\| x \|$ in terms of $\| y \|_+$, namely,

LEMMA 4. *If $y \in B_1^+ - I_+$ and if x is a pre-image of y, then*

$$\| x \|^{(1-\log r/\log r_{k+1})} \leqq (\tfrac{1}{2})^{\log r_1/\log r_{k+1}} (r_1 + r_n)/r_1 \cdot \| y \|_+ . \tag{12}$$

4. In this section, we will show how to bring every C^k mapping into a prepared form so that the considerations of the following section apply. To this end, we need the following well known lemma.

LEMMA 5. *Given a real formal power series $T = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ in n variables, there exists a C^∞ function ϕ having T as its Taylor series at the origin.*

Proof. Let $\alpha(x)$ be a C^∞ *function such that* $\alpha(x) \equiv 1$ for $x < \frac{1}{4}$ and $\alpha(x) = 0$ for $x > \frac{3}{4}$. Let $M_p = \sum_p \sum_{\Sigma i_j = p} (a_{i_1 \cdots i_n})$. The the function

$$\phi = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \alpha(p! M_p \| x \|^2)$$

satisfies the requirements of the lemma.

It follows from Lemma 5 that the natural projection ϕ_k of G^k onto F^k described in [6] is onto for all k, including the case $k = \infty$. Let T be an element of G^k satisfying the hypotheses of Theorem 1. Then $\phi_k(T)$ satisfies the hypotheses of Lemma 1 of [6], and hence, since ϕ_k is onto, we can find a C^k change of coordinates so that $\phi_k(T)$ is linear in the new coordinate system. Hence, we have proved

LEMMA 6. *Let T be an element of C^l and let L be the linear approximation to T at the origin. Then, by an appropriate change of coordinates, we can arrange that $T = L + F$, where*

$$F = (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$$

and the f's satisfy

$$f = o(\| x \|^{1/2}) \text{ if } l < \infty ; \; f = o(\| x \|^q) \text{ for all } q \text{ if } l = \infty . \tag{13}$$

If we examine the proof of Theorem 7 of [6], we see that, without destroying (11), we can arrange that I_+ and $I_- = \{x \mid \| x \|_- = 0\}$ are invariant surfaces and T reduces to the identity on I_+ and I_-. We have thus achieved the desired preliminary normalizations.

LEMMA 7. *If T satisfies the hypothesis of Theorem* 1, *then by a C^l*

change of coordinates it can be arranged that $T = L + F$, *where* F *satisfies* (13) *and vanishes on* I_+ *and* I_-.

5. In this section we shall complete the proof of Theorem 1. We first prove

LEMMA 8. *Let* f^* *be a* C^1 *function defined on* $C_1 \cap B_r$ *and such that* f^* *satisfies* (13). *Then there exists a function* $f \in C^1$ *satisfying* (13), *defined on* W_r *and reducing to* f^* *on* C_1 *and to* 0 *on* C.

Proof. Since C_1 is a smooth retract of W, we can certainly find an f^{**} of class C^1, defined on W_r, reducing to f^* on C and satisfying (13). If α denotes the functions of § 4, the function $f = \alpha([\| x \|_+ / \| x \|_-]^{\log \frac{1}{2}/\log(r_k/r_{k+1})} f^{**}$ satisfies the requirements of the lemma, where we set $f(0) = 0$.

Proof of Theorem 1. We wish to find a change of coordinates R which satisfies the functional equation

$$RL = TR. \tag{14}$$

Now if R were defined so as to satisfy (14) on W_r, then R could be extended to $L^m W_r$ by the simple device of $R(L^m x)$ to be $T^n R(x)$. By its very definition, R would be a smooth homeomorphism on all of $\bigcup_{m=-\infty}^{\infty} L^m W$ except possibly at the origin. We shall construct an R on W_r which can be extended to all of B_ϵ for sufficiently small positive ϵ.

We define R to be the identity on C. Then the functional equation (12) imposes no condition on R in W except on C_1. In terms of coordinates, if $R(x) = x_i + g_i(x_1, \cdots, x_n)$, (14) becomes

$$g_i(Lx) = f_i(x). \tag{15}$$

We can view (15) as defining g_i, and hence R, on C_1. The g's satisfy the hypotheses of Lemma 8, so that we can extend them to all of W_r so as to vanish on C and satisfy (13). Thus, for sufficiently small r, the mapping R will be a smooth homeomorphism at all points of W_r save the origin. By the remarks above, we can extend R to be a homeomorphism on all of $B_{\frac{1}{2}r}$ with the exception of I_+ and I_-. We would like to show that R with all its derivatives approaches the identity as a point goes to I_+ or I_-. Now R is getting more and more complicated in $L^m W_r$ as $m \to \infty$. In fact, for $y = L_x{}^m$ in $L^m W_r$, we have, by (14),

$$R(L^m x) = T^m R x = (L + F)^m R x. \tag{16}$$

But here, Lemma 3 comes to the rescue. In fact, although the expression for R gets more involved, the x occuring in (16) gets smaller and smaller. We can formalize the situation by introducing certain function spaces as in [6]. Let $G_\epsilon{}^q$ be the space of all C^q mappings of the form $G = (g_1, \cdots, g_n)$, where the g_i vanish at the origin with order q, which are defined on W_ϵ. On this space, we introduce the norm

$$\| G \|_\epsilon{}^l = \sup_{W_\epsilon} \sum_1^n \sum_{i_1+\cdots+i_n=l} (\partial g_i/\partial x_i{}^{i_1} \cdots \partial x_n{}^{i_n})^2, \tag{17}$$

where $l \leqq q$. It is clear that, given any $\delta > 0$ and any M, we can choose ϵ so small that

$$\| G \|_\epsilon{}^p \leqq (\delta/nM) \| G \|_\epsilon{}^l, \text{ for } p < l. \tag{18}$$

Now let D_T denote the operator on $G_\epsilon{}^q$ given by

$$D_T\colon G(\cdot) \to (L+F)(E+G)(\cdot\, r_{k+1}{}^{-1}\cdot) - L \cdot r_{k+1}{}^{-1}. \tag{19}$$

Then, since G admits a factor of $\| x \|^q$ and we can choose δ as small as we please, we have, given any α, for sufficiently large q,

$$\| D_T{}^G \|_\epsilon{}^l \leqq \alpha \| G \|_\epsilon{}^l + \| F \|_\epsilon{}^l. \tag{20}$$

In particular, we can choose $\alpha < r_n{}^{-l}$. Then, by Lemma 3, (16) and (20), we have that R approaches the identity with its first l derivatives as $m \to \infty$ if q is sufficiently large. Thus, at any point of I_+ and I_- other than the origin, R is of class C^l. At the origin, we can assume that the approach to the origin is through points of $L^m W^r$ with m bounded, since, for $M \to \infty$, $R \to E$. But then the estimates of Lemma 4 apply, since the expression for R is of one of a finite number of forms. Thus R can be defined on all of B_r, proving Theorem 1.

6. It should be noted that the estimates occurring in the proof of Theorem 1 depend, really, only on the ratios of the r_i. Thus, by Lemma 4 of [6], if T_t is a continuous one parameter group of transformations, it can be linearized provided the eigenvalues of a Jacobian (and hence of all Jacobians) at the origin satisfy (*). If we apply the considerations of Section 7 of [6], we obtain the following theorem on differential equations (which we state for, simplicity, in the C^∞ case).

THEOREM 2. *Let the system of differential equations*

$$dx_i/dt = X_i(x_1, \cdots, x_n) \tag{21}$$

be C^∞ and such that $X_i(0,\cdots,0)=0$. Let λ_i denote the eigenvalues of the matrix of linear terms of the X_i. Then if

(**) $\lambda_i \neq m_i\lambda_i$ *for any positive integral m_i with $m_i>1$,*

there exists a C^∞ change of coordinates linearizing (21).

This theorem is the C^∞ version of a well known result of Siegel [3]. It also generalizes to n dimensions the results of Birkhoff [1] in two dimensions and Birkhoff and Bamforth [2] for real eigenvalues in three dimensions, without their unnatural analyticity requirements.

7. In this section we wish to consider what happens when (*) is violated. We still retain, however, condition (1). In fact, if (1) were violated and some eigenvalue were of absolute value one, then the linear term is stable (on some lower dimensional invariant surface) and cannot be indicative of what happens in the non-linear case. We also note that the considerations of § 3 apply to non-linear as well as to linear transformations, provided that a small modification is made in all of the constants occurring in the lemmas. We shall asume, for simplicity, that the eigenvalues s_i are real; complex eigenvalues add no essential difficulties. Let M_i denote the set of n-tuples of positive integers $(m_1,\cdots,m_n)$ such that

$$s_i = {s_i}^{m_1}\cdots{s_n}^{m_n}. \tag{22}$$

If m and m^* are two elements of M_i, then $m-m^*\in S$, where S is the group of those n-tuples $(m_1,\cdots,m_n)$ such that

$$1 = {s_1}^{m_1}\cdots{s_n}^{m_n}. \tag{23}$$

Then choosing a basis B for the positive elements of S, we can express all but a finite number of elements of M_i as products of some one element m and multpiles of elements of B. Combining these considerations with Lemma 9 of [6] and Lemma 5 above, we obtain

THEOREM 3. *Let T be a C^∞ local mapping whose eigenvalues at the origin satisfy* (1). *Then there exist a finite number of monomials depending only on the eigenvalues, such that T is equivalent to a transformation of the form $L+F$, where L is linear and F depends only on the P_j's.*

For example, if $n=2$ and $s_1=s_2^{-1}$, we can find a change of coordinates so that T has the form

$$x_1 = sx + xf(xy), \qquad y_1 = s^{-1}y + yg(xy).$$

THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] G. D. Birkhoff, "Divergente Reihen und singuläre Punkte gewöhnlicher Differentialgleichungen," *Berliner Sitzungsberichte der Preussischen Akademie der Wissenschaften*, 1929, pp. 1-15.

[2] ——— and F. R. Bamforth, "Divergent series and singular points of ordinary differential equations," *Transactions of the American Mathematical Society*, vol. 32 (1930), pp. 114-146.

[3] C. L. Siegel, "Über die Normalform analytischer Differentialgleichungen in der Nähe einer Gleichgewichtslösung," *Göttinger Nachrichten der Akademie der Wissenschaften*, 1952, pp. 21-30.

[4] S. Sternberg, "On the behavior of invariant curves near a hyperbolic point of a surface transformation," *American Journal of Mathematics*, vol. 75 (1955), pp. 526-534.

[5] ———, "On local C^n contractions of the real line," *Duke Mathematical Journal*, vol. 24 (1957), pp. 97-102.

[6] ———," Local contractions and a theorem of Poincaré," *American Journal of Mathematics*, vol. 79 (1957), pp. 809-824.

ON THE PONTRYAGIN CLASSES OF CERTAIN $SO(n)$-BUNDLES OVER MANIFOLDS.*

By MICHEL A. KERVAIRE.

One of the main steps in the proof of the well known

THEOREM (Rochlin [4]). *If $w_2(M_4) = 0$, then $p_1(M_4)$ is divisible by* 48, is the following lemma due to Pontryagin who stated it without proof in the Doklady Akademii Nauk S.S.S.R., XLVII, N. 5, pp. 327-330. (In Rochlin's theorem, $w_2(M_4)$ is the 2-dimensional Stiefel-Whitney class of the 4-dimensional, orientable, closed, differentiable manifold M_4 and $p_1(M_4)$ the first (4-dimensional) Pontryagin class of M_4.)

LEMMA. *Let the closed differentiable manifold M_4 of dimension* 4 *be the base space of a principal $\boldsymbol{SO}(n)$-bundle $\mathfrak{N}$. Assume that $\mathfrak{N}$ admits a cross-section over the subset $M - U$ of M, where U is a spherical neighborhood of some point in M_4. Let $\lambda \in \pi_3(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$ be the integer representing, up to sign, the obstruction to the extension over M of the cross-section given over $M - U$. Then, $p_1(M_4) = 2\lambda$, up to sign.*

A tentative method toward generalizing Rochlin's theorem starts with generalizing this lemma. This is done below. I do not know whether this will actually lead to a reasonable generalization of Rochlin's theorem. However, the generalized lemma might have some interest in itself.

I am indebted to A. Borel for valuable discussions during the preparation of the present paper.

1. Let M_{4s} be a closed manifold of dimension $4s$. Let $\mathfrak{N}$ be a principal $\boldsymbol{SO}(n)$-bundle over M_{4s} which admits a cross-section over $M - U$. We shall say for brevity that the bundle $\mathfrak{N}$ is "*almost trivial.*" Assume that $4s < n$ and let λ denote the integer representing the homotopy class in $\pi_{4s-1}(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$ (see [1]) of the obstruction to the extension over M_{4s} of the cross-section given over $M - U$. All manifolds considered in this paper are assumed to be orientable.

* Received January 10, 1958.

LEMMA (1.1). *The value on M_{4s} of the $4s$-dimensional Pontryagin class p_s of the bundle $\mathfrak{N}$ is given by the formula: $p_s[M_{4s}] = a_s \cdot \lambda \cdot (2s-1)!$, up to sign, where a_s is equal to 1 or 2 according to whether s is even or odd respectively.*

Results concerning the same question in the non-stable range ($n < 4s+1$) can be deduced (using Lemma (3.1) below) from results in a forthcoming paper by A. Borel and F. Hirzebruch: "On the characteristic classes of homogeneous spaces."

Before we proceed to the proof of the above lemma, let us recall briefly the argument by which it implies Rochlin's theorem:

2. Let the orientable, closed, differentiable manifold M_4 be imbedded in euclidean $(n+4)$-space E_{n+4} in such a way that U is the hemisphere $x_0 \leqq 0$ of the unit sphere $S_4 \subset E_5 \subset E_{n+4}$. Assume that $M - U$ lies in $\{x_0 \geqq 0\}$ and that the imbedding of M_{4s} in E_{n+4} is differentiable of class C^2. The assumption $w_2(M_4) = 0$ is equivalent to the existence of a field of n-frames $\boldsymbol{F}_n$ defined over $M - U$ and orthogonal to M_4 in E_{n+4} (because M_4 was assumed to be orientable and $\pi_2(\boldsymbol{SO}(n)) = 0$). By Lemma (1.1), $\bar{p}_1[M_4] = 2\lambda$, where $\bar{p}_1$ is the 4-dimensional Pontryagin class of the normal bundle over M_4 in E_{n+4}. The integer λ represents the homotopy class of the mapping $\mu: S_3 \to \boldsymbol{SO}(n)$ which sends a point $x \in U$ (identified with S_3) into the matrix of components of the vectors of $\boldsymbol{F}_n$ at x relative to the vectors at x of some field of normal n-frames over S_4 in E_{n+4} (Take for instance the field consisting of the normal to S_4 in E_5 followed by the vectors of an orthonormal basis of the orthogonal complement of E_5 in E_{n+4}). By the interpretation of J (the Hopf's homomorphism) given in [2] and the fact that $\boldsymbol{F}_n \mid U$ can be extended over $M - U$, it follows that the element $J\mu \in \pi_{n+3}(S_n)$ is zero. Since $J\pi_3(\boldsymbol{SO}(n)) = \pi_{n+3}(S_n) \approx \boldsymbol{Z}_{24}$, it follows that λ is divisible by 24. Consequently $\bar{p}_1[M_4]$ is divisible by 48. By Whitney duality (which holds over the integers in this special case), we have $p_1[M_4] = -\bar{p}_1[M_4]$. Hence the theorem.

3. Using the following lemma, we reduce the study of almost trivial bundles over a closed manifold M_d to the study of bundles over the sphere S_d:

LEMMA (3.1). *Let $f: M_d \to B_G$ be a mapping of M_d into the classifying space for G and assume that the induced principal $\boldsymbol{G}$-bundle over M_d is almost trivial* (i.e., *admits a cross-section over $M - U$*). *Then f is homo-*

topic to a composite map $f' \circ \alpha$, where $\alpha: M_d \to S_d$ has degree 1 and f' maps S_d into B_G.

Proof of lemma (3.1). Denote by $\pi: E_G \to B_G$ the projection in the classifying fibration. Since the bundle over M_d induced by f is almost trivial, there exists a mapping $F: M - U \to E_G$, such that $\pi \circ F = f \mid M - U$. We may assume that f is constant on U: $f(U) = b \in B_G$. The map F is homotopic to zero (E_G is contractible). Let F_t be a homotopy: $F_0 = F$, F_1 maps $M - U$ into some points of E_G. It is convenient for later purposes to assume that $F_t = F$ for $0 \leqq t \leqq \frac{1}{2}$. Introduce generalized polar coordinates (x, r) in U ($x \in U$, $r =$ distance from (x, r) to the center of U). The required homotopy between f and a map of the form $f' \circ \alpha$ is given by

$$f_t(z) = \pi F_t(z) \qquad \text{for } z \in M - U,$$

$$f_t(x, r) = \pi F_{tr}(x, 1) \quad \text{for } (x, r) \in U$$

(We take the radius of U to be 1).

Clearly, $f_t(z)$ is continuous in both z and t. We verify that $f_0 = f$: for

$z \in M - U$, $f_0(z) = \pi F_0(z) = \pi F(z) = f(z)$; for

$(x, r) \in U$, $f_0(x, r) = \pi F_0(x, 1) = \pi F(x, 1) = f(x, 1) = f(x, r) = b$.

For $t = 1$, we have

$$f_1(z) = \pi F_1(z) = b' \text{ a constant point } (z \in M - U),$$

$$f_1(x, r) = \pi F_r(x, 1).$$

Clearly, f_1 has the form $f' \circ \alpha$, where $\alpha: M_d \to S_d$ shrinks $M - U$ into a point and maps the interior of U homeomorphically into S_d (thus α has degree 1), and f' sends $\alpha(x, r)$ into $\pi F_r(x, 1)$.

4. Let $f: M_{4s} \to B_{SO(n)}$ induce an almost trivial bundle over M_{4s} ($4s + 1 < n$). We may assume, without loss of generality, that the section over $M - U$ is given by a mapping $F: M - U \to E_{SO(n)}$ (such that $\pi F = f \mid M - U$). Assuming for convenience as in § 3 that $f(U) = b \in B_{SO(n)}$, $F \mid U$ defines a mapping of S_{4s-1} into $\boldsymbol{SO}(n)$. Since we assumed $4s + 1 < n$, one has by [1], $\pi_{4s-1}(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$. Let λ be the integer (determined up to sign) representing the homotopy class of $F \mid U$ in $\boldsymbol{SO}(n)$. Denote by

$p_s \in H^{4s}(M_{4s}; \mathbf{Z})$ the Pontryagin class of dimension $4s$ of the $\boldsymbol{SO}(n)$-bundle over M_{4s} induced by f. We have to prove that $p_s[M_{4s}] = a_s \cdot \lambda \cdot (2s-1)!$.

Let $f' \circ \alpha \simeq f$ be the factorization given by Lemma (3.1). Denote by χ the characteristic map of the bundle over S_{4s} induced by f'. We shall prove (up to sign):

(1) $\chi = \lambda$, (we use also χ to denote the integer representing the homotopy class of χ),

(2) $p_s[M_{4s}] = p'[S_{4s}]$, where p'_s is the $4s$-dimensional Pontryagin class of the bundle over S_{4s} induced by f'.

(3) $p'_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)!$.[1]

Proof of (1). Define $F' : S_{4s} - V \to E_{\boldsymbol{SO}(n)}$ by $F'(\alpha(x,r)) = F_r(x,1)$, where V is the image by α of the set of those $(x,r) \in U$ with $0 \leqq r \leqq \frac{1}{2}$. Since we assumed $F_t = F$ for $0 \leqq t \leqq \frac{1}{2}$ (see § 3), $\pi F'(V) = \pi F(U_{\frac{1}{2}}) = f(U_{\frac{1}{2}}) = b$, where $U_{\frac{1}{2}}$ is the set of points $(x, \frac{1}{2}) \in U$. On the other hand, $\pi F' = f' \mid S_{4s} - V$. In other words, $F' \mid V$ defines a mapping $S_{4s-1} \to \boldsymbol{SO}(n)$ which is precisely the characteristic map χ of the bundle over S_{4s} induced by f' (we use χ for the map and its homotopy class). But $F'(x, \frac{1}{2}) = F_{\frac{1}{2}}(x,1) = F(x,1)$. This means that χ is also represented by $F \mid U$. Hence $\chi = \lambda$.

Proof of (2). Trivial by naturality of the Pontryagin classes (and the fact that α has degree 1).

Proof of (3). We are left with the following situation: Let $(E, \boldsymbol{SO}(n), S_{4s})$ be a principal $\boldsymbol{SO}(n)$-bundle over S_{4s} and χ its characteristic map. $\chi = \partial i_{4s}$, where ∂ is the boundary operator in the homotopy sequence of $\pi : E \to S_{4s}$. Let p_s be the $4s$-dimensional Pontryagin class of $(E, \boldsymbol{SO}(n), S_{4s})$. We have to prove:

$$p_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)!$$

(up to sign).

Let $\alpha : \boldsymbol{SO}(n) \to \boldsymbol{U}(n)$ be the standard injection and denote by c_{2s} the $4s$-dimensional Chern class of the extended bundle $(E', \boldsymbol{U}(n), S_{4s})$. By definition $p_s[S_{4s}] = c_{2s}[S_{4s}]$ up to sign. It is well known that $\pi_{4s-1}(W_{n,n-2s+1}) \simeq \mathbf{Z}$. We have $\partial_A i_{4s} = c_{2s}[S_{4s}] \cdot \epsilon_W$, where $\partial_A : \pi_{4s}(S_{4s}) \pi_{4s-1}(W_{n,n-2s+1})$ is the boundary operator of the homotopy sequence of the fibration with fibre $W_{n,n-2s+1}$ associated with $(E', \boldsymbol{U}(n), S_{4s})$ and ϵ_W is a generator of $\pi_{4s-1}(W_{n,n-2s+1})$.

To evaluate $c_{2s}[S_{4s}]$, consider the commutative diagram

[1] The divisibility of $p'_s[S_{4s}]$ by $(2s-1)!$ is also known to R. Bott.

$$\begin{array}{ccccc}
\pi_{4s-1}(\boldsymbol{SO}(n)) & \xrightarrow{\alpha_*} & \pi_{4s-1}(\boldsymbol{U}(n)) & \xrightarrow{q_*} & \pi_{4s-1}(W_{n,n-2s+1}) \\
\uparrow{\scriptstyle \partial} & & \uparrow & & \uparrow{\scriptstyle \partial_A} \\
\pi_{4s}(S_{4s}) & \xrightarrow{\text{identity}} & \pi_{4s}(S_{4s}) & \xrightarrow{\text{identity}} & \pi_{4s}(S_{4s}),
\end{array}$$

where $q: \boldsymbol{U}(n) \to W_{n,n-2s+1}$ is the natural projection. Using the definition of $c_{2s}[S_{4s}]$, we get

$$c_{2s}[S_{4s}] \cdot \epsilon_W = \partial_A(i_{4s}) = q_*\alpha_*\partial(i_{4s}) = \chi q_*\alpha_*\epsilon_{8s} = a_s \cdot \chi \cdot q_*\epsilon_U,$$

where χ denotes also the integer representing the homotopy class of χ.

Consider the homotopy sequence of the fibration $\boldsymbol{U}(n)/\boldsymbol{U}(2s-1) = W_{n,n-2w+1}$ with projection q:

$$\cdots \to \pi_{4s-1}(\boldsymbol{U}(n)) \longrightarrow \pi_{4s-1}(W_{n,n-2s+1}) \to \pi_{4s-2}(\boldsymbol{U}(2s-1)) \to \pi_{4s-2}(\boldsymbol{U}(n)).$$

By R. Bott, $\pi_{4s-2}(\boldsymbol{U}(n)) = 0$ and $\pi_{4s-2}(\boldsymbol{U}(2s-1)) = \boldsymbol{Z}/(2s-1)!\boldsymbol{Z}$. Therefore, q_* is the multiplication by $(2s-1)!$ (precisely, $q_*\epsilon_U = (2s-1)!\epsilon_W$). It follows that

$$p_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)!,$$

up to sign. It was proved in [3], Lemma 3, that $a_{2k+1} = 2$ and $a_{2k} = 1$. This completes the proof of Lemma (1.1).

5. *Remarks.* The same method gives the Chern class c_s of an almost trivial $\boldsymbol{U}(n)$-bundle over a $2s$-dimensional manifold ($s \leqq n$) and similarly the symplectic Pontryagin class e_s of an almost trivial $\boldsymbol{Sp}(n)$-bundle over a $4s$-dimensional manifold (for the "symplectic" Pontryagin classes, see A. Borel and F. Hirzebruch, loc. cit., Chapter I, 9.6).

LEMMA (5.1). *Let M_{2s} be the base space of an almost trivial principal $\boldsymbol{U}(n)$-bundle $\mathfrak{N}$. Let $\lambda(F)$ be the obstruction to the extension M_{2s} of a cross-section F in $\mathfrak{N}$ given over $M - U$ ($\lambda(F) \in \pi_{2s-1}(\boldsymbol{U}(n))$). Assume $s < n$, thus $\pi_{2s-1}(\boldsymbol{U}(n)) \approx \boldsymbol{Z}$. Let c_s denote the $2s$-dimensional Chern class of $\mathfrak{N}$. We have $c_s[M_{2s}] = (s-1)!\lambda(F)$.*

Similarly, let M_{4s} be the base space of an almost trivial $\boldsymbol{Sp}(n)$-bundle $\mathfrak{N}$. Assume $s < n$, then the obstruction to the extension over M of a cross-section defined over $M - U$ (U some spherical neighborhood in M) can be represented by an integer $\lambda(\pi_{4s-1}(\boldsymbol{Sp}) \approx \boldsymbol{Z}$ by R. Bott [1]). Let σ be the standard

inclusion $\sigma: \boldsymbol{Sp}(n) \to \boldsymbol{U}(2n)$ and $\sigma^*: H^*(B_{\boldsymbol{U}(2n)}) \to H^*(B_{\boldsymbol{Sp}(n)})$ the induced homomorphism in integral cohomology of the classifying spaces. The symplectic Pontryagin classes of an $\boldsymbol{Sp}(n)$-bundle induced by a mapping $f: M \to B_{\boldsymbol{Sp}(n)}$ are, up to sign, the images by $f^* \circ \sigma^*$ of the universal Chern classes $C_{2i} \in H^{4i}(B_{\boldsymbol{U}(2n)})$.

LEMMA (5.2). *Let e_s denote the $4s$-dimensional symplectic Pontryagin class of $\mathfrak{R}$. We have $e_s[M_{4s}] = b_s \cdot \lambda \cdot (2s-1)!$, where b_s is equal to 1 if s is odd, to 2 if s is even.*

The proofs are entirely similar to the one of Lemma (1.1) and are left to the reader. For the proof of Lemma (5.2), one has to use that $\sigma_*: \pi_{4s-1}(\boldsymbol{Sp}(n)) \to \pi_{4s-1}(\boldsymbol{U}(2n))$ maps a generator into b_s-times a generator, a fact which follows from [1], formula (3.6) and the knowledge of the stable homotopy groups of $\boldsymbol{Sp}(n)$.

We have two more remarks: in the situations of Lemmas (1.1), (5.1) and (5.2), it follows that $\lambda(F)$, the obstruction to the extension of the partial cross-section F, does not depend on F, a fact which could also be proved directly (the Hurewicz homomorphisms

$$\pi_{2s-1}(\boldsymbol{U}(n)) \to H_{2s-1}(\boldsymbol{U}(n)), \qquad \pi_{4s-1}(\boldsymbol{SO}(n)) \to H_{4s-1}(\boldsymbol{SO}(n)),$$

$$\pi_{4s-1}(\boldsymbol{Sp}(n)) \to H_{4s-1}(\boldsymbol{Sp}(n))$$

are monomorphisms[2] for large n).

Finally, we notice that R. Bott's result: $\pi_{2n}(\boldsymbol{U}(n)) \approx \boldsymbol{Z}/n!\boldsymbol{Z}$ which was used in both Lemmas (1.1) and (5.2) implies

(5.3) $\qquad \pi_{4s-2}(\boldsymbol{Sp}(s-1)) \approx \boldsymbol{Z}/b_s(2s-1)!\boldsymbol{Z}$. ($b_s$ as in Lemma (5.2)).

Indeed, the projection k_* in the homotopy sequence

$$\cdots \to \pi_{4s-1}(\boldsymbol{Sp}(s)) \xrightarrow{k_*} \pi_{4s-1}(S_{4s-1}) \to \pi_{4s-2}(\boldsymbol{Sp}(s-1)) \to \pi_{4s-2}(\boldsymbol{Sp}(s))$$

is the composition $k_* = q_* \circ \sigma_*$, where $\sigma_*: \pi_{4s-1}(\boldsymbol{Sp}(s)) \to \pi_{4s-1}(\boldsymbol{U}(2s))$ is induced by the standard inclusion $\sigma: \boldsymbol{Sp}(s) \to \boldsymbol{U}(2s)$ and $q_*: \pi_{4s-1}(\boldsymbol{U}(2s)) \to \pi_{4s-1}(S_{4s-1})$ is induced by the projection $q: \boldsymbol{U}(2s) \to S_{4s-1}$. Now, σ_* sends generator into b_s-times generator and q_* sends generator into $(2s-1)!$-times generator. Therefore, k_* sends a generator of $\pi_{4s-1}(\boldsymbol{Sp}(s)) \approx \boldsymbol{Z}$ into $b_s \cdot (2s-1)!$ times a generator of $\pi_{4s-1}(S_{4s-1})$. Since $\pi_{4s-2}(\boldsymbol{Sp}(s)) = 0$, we have $\pi_{4s-2}(\boldsymbol{Sp}(s-1)) \approx \pi_{4s-1}(S_{4s-1})/k_*\pi_{4s-1}(\boldsymbol{Sp}(s))$. Hence (5.3).

THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] R. Bott, "The stable homotopy of the classical groups," *Proceedings of the National Academy of Sciences*, vol. 43 (1957), pp. 933-935.

[2] M. Kervaire, "An interpretation of G. Whitehead's generalization of Hopf's invariant," to appear.

[3] ———, "Non-parallelizability of S_n for $n > 7$," *Proceedings of the National Academy of Sciences*, vol. 44 (1958), pp. 280-283.

[4] W. Rochlin, "Classification of mappings of S_{n+3} onto S_n," *Doklady Akademii Nauk S.S.S.R.*, vol. 81 (1951).

ON THE λ-VARIANT OF MERTENS' μ-HYPOTHESIS.*

By AUREL WINTNER.

Let $M(n)$, $L(n)$; $J(n)$, $K(n)$ denote the n-th partial sums of the series $\Sigma\mu(n)$, $\Sigma\lambda(n)$; $\Sigma\mu(n)/\sqrt{n}$, $\Sigma\lambda(n)/\sqrt{n}$ respectively, where $\mu(n)$ and $\lambda(n)$ are Möbius' and Liouville's factors, defined by $1/\zeta(s) = \Sigma\mu(n)/n^s$ and $\zeta(2s)/\zeta(s) = \Sigma\lambda(n)/n^s$. According to Littlewood, the convergence of either (or both) of the latter series for $s > \frac{1}{2}$ is equivalent to Riemann's hypothesis (= R. H.). According to Landau, the unilateral boundedness of any one of the functions $M, \cdots, K$ of n implies, without being implied by, R. H. In particular, more than R. H. is implied (for trivial reasons) not only by Mertens' hypothesis

$$M(n) = O(\sqrt{n}), \quad \text{where } M(n) = \sum_{m=1}^{n} \mu(m), \tag{1}$$

but also by Pólya's hypothesis (= P. H.), which claims that $L(n) \leqq 0$ (or even $L(n) < 0$) holds for every $n > 1$ (or $n > 2$); for references and certain conclusions cf. a paper of Ingham [1] (and, concerning a λ-hypothesis which is distinct from P. H. and was propounded by Turán, the recent conclusions of S. Selberg [2].

Neither the necessity nor the sufficiency of (1) for P. H. is known (and, what is more curious, no implicative connection is known between Pólya's and Turán's λ-hypotheses). On the other hand, the formal λ-analogue of (1) is not P. H. but

$$L(n) = O(\sqrt{n}), \quad \text{where } L(n) = \sum_{m=1}^{n} \lambda(m). \tag{2}$$

I do not know of an implicative connection between either (1) or P. H. (or, for that matter, S. Selberg's version of Turán's hypothesis) on the one hand, and the hypothesis (2), which does not seem to have been considered in the literature, on the other hand. But something *like* P. H. (a certain "negative preponderance" of the same type as P. H.) can be expected to follow from (2), and even from R. H., which claims less than (2). Such an expectation rests on the circumstance that

$$\operatorname*{res}_{s=\frac{1}{2}} \zeta(2s)/\zeta(s) < 0. \tag{3}$$

* Received May 14, 1958.

As a matter of fact, the available numerical evidence for the truth of P.H. could be *merely a reflection of* (3). [Needless to say, (3) follows not only from the value of $\zeta(\frac{1}{2})$ but, more immediately, from the circumstance that, whereas $\zeta(2s)$ does not change sign when s passes from $s>1$ to $s<1$, the function $\zeta(s)$, having a *simple* pole at $s=1$, must change sign at $s=1$ on the real axis.]

Actually, while (3) does not seem to be able to lead from (2) to a "negative preponderance" in terms of $L(n)$ (which is P.H.), it does lead to a "negative preponderance" in terms of $K(n)$. In fact, (2) turns out to imply that

$$K(n)/\log n \to c, \quad \text{where } K(n)=\sum_{m=1}^{n}\lambda(m)/\sqrt{m}, \tag{4}$$

holds for a certain *negative* constant c, and so $K(n)\to-\infty$. But much more than (4) can be concluded if an argument applied to (1) in an earlier note [3] is adapted to (2).

Consider the following refinement (1*) of (1):

$$J(n)=O(1), \quad \text{where } J(n)=\sum_{m=1}^{n}\mu(m)/\sqrt{m}. \tag{1*}$$

A partial summation shows that (1*) implies (1). On the other hand, a partial summation fails to lead from (1) to (1*). In fact,

$$[\sum_{m=1}^{n}c_m=O(\sqrt{n})]\Rightarrow[\sum_{m=1}^{n}c_m/\sqrt{m}=O(\log n)]$$

for arbitrary $c_1, c_2, \cdots$ but, as shown by the example $c_n=1/\sqrt{n}$, nothing more can in general be concluded. But the $O(\log n)$ can be improved to $O(1)$ in the particular case $c_n=\mu(n)$, which means that (1) is equivalent to (1*). As shown in [3], this follows for function-theoretical Tauberian reasons. Since the truth of (1*) appears to be quite unlikely (it may or, in contrast with (1), it may not at all, be indicated by the beginning of a numerical table), the usual "theoretical" objection against Mertens' hypothesis appears in a strengthened form.

It turns out that the "theoretical" objection to (2) can be straightened correspondingly, and in a manner which appears to be even more striking (though actually it is not). In fact, *the following relation* (2*) *proves to be equivalent to* (2):

$$K(n)=c\log n+O(1), \quad \text{where } K(n)=\sum_{m=1}^{n}\lambda(m)/\sqrt{m} \tag{2*}$$

(here c denotes, as in (4), a certain negative constant). This speaks much against (2), since the truth of anything like (2*) seems to be unlikely.

Proof of (2*) $\Rightarrow$ (2). This requires nothing but a partial summation (no matter what the given value of c may be).

Proof of (2) $\Rightarrow$ (2*). In [3], the proof of (1) $\Rightarrow$ (1*) resulted, on the one hand, from the fact that

(i) the function $1/\zeta(s)$ is regular at the point $s=\frac{1}{2}$, and, on the other hand, from an application of

(ii) a lemma Tauberian in nature, representing an *O-variant* of M. Riesz' *convergence* theorem concerning Dirichlet series (the convergence theorem which extends Fatou's theorem on power series to Dirichlet series).

Condition (i) becomes violated if the function $1/\zeta(s)$, occurring in (i), is replaced by the function $\zeta(2s)/\zeta(s)$, since the latter has a pole at $s=\frac{1}{2}$. This pole can, however, be eliminated if $\zeta(2s)/\zeta(s)$ is replaced by the sum $\gamma(s)$ defined by

$$\gamma(s)=\zeta(2s)/\zeta(s)-c\zeta(s+\tfrac{1}{2}), \tag{5}$$

where c is a constant, to be determined by the condition that the simple pole possessed at $s=\frac{1}{2}$ by the first term of (5) be compensated by the simple pole possessed at $s=\frac{1}{2}$ by the second term of (5). Accordingly, condition (i) is satisfied if the function $1/\zeta(s)$ is replaced by the function (5), where $c<0$, by (3).

Since

$$\zeta(2s)/\zeta(s)=\sum_{n=1}^{\infty}\lambda(n)/n^s \text{ and } \zeta(s)=\sum_{n=1}^{\infty}1/n^s,$$

it is seen from (5) that the series

$$1/\zeta(s)=\sum_{n=1}^{\infty}\mu(n)/n^s \tag{6}$$

must be replaced by the series

$$\gamma(s)=\sum_{n=1}^{\infty}[\lambda(n)-c/\sqrt{n}]/n^s. \tag{7}$$

But what corresponds to the hypothesis (1) for the Dirichlet series (6) is the hypothesis

$$\sum_{m=1}^{n}[\lambda(m)-c/\sqrt{m}]=O(\sqrt{n}) \tag{8}$$

for the Dirichlet series (7). Consequently, if the Tauberian lemma, referred to under (ii), is used in precisely the same way as it was used in the proof of (1) $\Rightarrow$ (1*) in [3], then, since what now corresponds to (1*) is the estimate

$$\sum_{m=1}^{\infty} [\lambda(m) - c/\sqrt{m}]/\sqrt{m} = O(1), \tag{9}$$

there results the truth of the (unconditional) implication (8) $\Rightarrow$ (9).

Finally,

$$\sum_{m=1}^{n} 1/\sqrt{m} = O(\sqrt{n}) \text{ and } \sum_{m=1}^{n} (c/\sqrt{m})/\sqrt{m} = c \log n + O(1)$$

(the $O(1)$ claims less than the existence of the Euler-Mascheroni constant). Hence, (8) and (9) are equivalent to (2) and (2*) respectively. Consequently, (8) $\Rightarrow$ (9) is equivalent to (2) $\Rightarrow$ (2*). Since (8) $\Rightarrow$ (9) was just proved, the proof of (2) $\Rightarrow$ (2*) is complete.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] A. E. Ingham, "On two conjectures in the theory of numbers," *American Journal of Mathematics*, vol. 64 (1942), pp. 313-319.

[2] S. Selberg, "Über eine Vermutung von P. Turán," *Det Kongelige Norske Videnskabers Selskabs Forhandlinger*, vol. 29 (1956), pp. 33-35.

[3] A. Wintner, "A note on Mertens' hypothesis," *Revista de Ciencias* (Lima), vol. 50 (1948), pp. 181-184.

PARTITIONS OF LARGE BIPARTITES.*

By E. M. WRIGHT.

1. In a recent article [4], I found an asymptotic formula for the number of partitions of a bi-partite number (m, n) whose components m, n are large but of the same order, i.e., their ratio is bounded above and below. I also gave without proof the first few terms of an asymptotic formula for the logarithm of the number of partitions of a multi-partite number $(n_1, n_2, \cdots, n_j)$, the ratios of whose components are all bounded below. Just before the article appeared, I found that Auluck [1] had dealt with one of my four cases for bipartites, under the same condition, and that Meinardus [2] had found the first term of my formula for multi-partites. Auluck indicates that his results for bi-partites (and any results obtainable for multi-partites) have applications to the study of the thermodynamical properties of assemblies characterised by the conservation of two or more parameters. He found an entirely different result true when m is fixed and n large, and Nanda [3] has shown that this is true for $m = o(n^{\frac{1}{3}})$.

A much more precise approximation for the generating function has now been found [6], and this enables me to deal here with all large m and n such that

$$\tfrac{1}{2} + \epsilon_1 < \log n / \log m < 2 - \epsilon_2 \tag{1.1}$$

for any fixed positive ϵ_1, ϵ_2. This is a substantial relaxation of the restriction imposed in both [1] and [4] that m/n should be bounded above and below.

Auluck's result and the result in two of my four cases involved a definite integral $I(m/n)$ which neither of us was then able to evaluate (except that Auluck evaluated $I(1)$). This problem has since been solved [5], and I use the results here.

2. Notation and Result. A *bi-partite number* (m, n) is a two-dimensional vector whose components m, n are non-negative rational integers. A *partition* of (m, n) is a solution of the vector equation

$$\sum_k (m_k, n_k) = (m, n) \tag{2.1}$$

* Received January 6, 1958.

in bi-partite numbers other than $(0,0)$; two partitions are regarded as identical if they differ only in the order of the bi-partite numbers on the left of (2.1). We write $p^{(1)}(m,n)$ for the number of partitions of (m,n) and $p^{(2)}(m,n)$ for the number of such partitions in which no part has a zero component. Again, we write $p^{(3)}(m,n)$ for the number of partitions of (m,n) into *different* parts and $p^{(4)}(m,n)$ for the number of partitions into different parts, no one of which has a zero component. Our object is to find an asymptotic formula for $p^{(s)}(m,n)$ for large m and n satisfying (1.1).

In what follows, $s=1,2,3$ or 4; any statement involving s is true for these four values of s. The letter s is frequently omitted, so that, for example, $p(m,n)$ is written for $p^{(s)}(m,n)$, a for $a^{(s)}$, and so on.

We write

$$a^{(1)}=a^{(2)}=\zeta(3)=\sum_{r=1}^{\infty}r^{-3}=1.20205690\cdots,$$

$$a^{(3)}=a^{(4)}=(3/4)\zeta(3),\quad b^{(1)}=-b^{(2)}=\pi^2/12,\quad b^{(3)}=-b^{(4)}=\pi^2/24,$$

and γ for Euler's constant, so that

$$\gamma=\lim_{r\to\infty}(1+1/2+1/3+\cdots+1/r-\log r)=0.5772157\cdots.$$

Again, for all complex z such that $\Re(z)>0$, we write

$$c^{(2)}(z)=(z+3+z^{-1})/24,\quad c^{(1)}(z)=c^{(2)}(z)-\tfrac{1}{2},\quad c^{(3)}(z)=c^{(4)}(z)=0,$$

and

$$I(z)=\int_0^{\infty}\{(u(e^{zu}-1)(e^u-1))^{-1}-z^{-1}u^{-3}+\tfrac{1}{2}(1+z^{-1})u^{-2}-2c_2(z)(e^u-1)^{-1}\}du.$$

It is readily verified that this integral converges. Its evaluation is discussed in [5]. In particular, if $n=o(m)$, we have

$$I(n/m)=\alpha_{-1}m/n+\alpha_0+O(n^3/m^3), \tag{2.2}$$

where $\alpha_{-1}=(1-\gamma)/12-\zeta'(-1)=.20065317\cdots,$

$$\alpha_0=\tfrac{1}{4}\log(2\pi)-\tfrac{1}{4}\gamma=.31516535\cdots.$$

We write also

$$d^{(2)}(z)=c^{(2)}(z)(\log z+2\gamma)+I(z),$$

where $\log z$ has its principal value, and

$$d^{(1)}(z)=d^{(2)}(z)-\log 2\pi,\quad d^{(3)}=2c^{(1)}\log 2,\quad d^{(4)}=2c^{(2)}\log 2,$$

$$D(z)=d(z)-\log(2\pi a3^{\frac{1}{2}})-b^2(z-1+z^{-1})/3a.$$

A little calculation shows that $d^{(2)}(1/z) = d^{(2)}(z)$, and a similar result follows trivially for c, $d^{(1)}$, $d^{(3)}$, $d^{(4)}$ and D.

The numbers ϵ, ϵ_1, ϵ_2 are positive numbers, to be thought of as small. C is a positive number, not always the same at each occurrence, which may depend upon any of ϵ, ϵ_1, ϵ_2, s, h, k, but not on m, n, x, y, X, Y, θ, ϕ, ξ, η, u, t, z. The symbols $O(\ )$ and $o(\ )$ refer to the passage of m and n to infinity or of x, y, X, Y to zero. The constant implied in the $O(\ )$ notation is of type C and all statements are subject to the implied conditions "for $m > C$ and $n > C$" or "for $|x| < C$ and $|y| < C$," as may be appropriate.

We write

$$\mu = (amn^{-2})^{\frac{1}{3}}, \qquad \nu = (anm^{-2})^{\frac{1}{3}}, \tag{2.3}$$

so that, when (1.1) is satisfied, μ and ν are $o(1)$. We shall repeatedly make use of the relations

$$\mu^3\nu^3 = a^2/mn, \qquad \nu/\mu = n/m. \tag{2.4}$$

We write $T_1(t) = 0$ and

$$T_H(t) = a\sum_{h=3}^{2H-1} P_h t^{h-1} \qquad (H \geqq 2),$$

where $P_h^{(1)}$ and $P_h^{(2)}$ are polynomials in $\log t$ of degree $[\frac{1}{2}h]$, whose coefficients can be calculated, and $P_h^{(3)}$ and $P_h^{(4)}$ are numbers depending only on h and s. In particular,

$$P_h^{(2)} = (-1)^h P_h^{(1)}, \qquad P_h^{(4)} = (-1)^h P_h^{(3)}.$$

We show how to calculate P_h in § 7 and give a table of P_h for $h \leqq 7$ at the end of the paper.

Our object is to prove the following

THEOREM. *If m and n tend to infinity subject to the condition* (1.1), *we have $p(m,n) \sim e^{\sigma}$, that is*

$$\log p(m,n) = \sigma + o(1),$$

where

$$\sigma = 3(amn)^{\frac{1}{3}} + b(m+n)/(amn)^{\frac{1}{3}} + (1/3)\{2 - c(n/m)\}\log(a^2/mn) + D(n/m) + \nu^{-1}T_K(\mu) + \mu^{-1}T_{K'}(\nu)$$

and

$$K = [3/8\epsilon_1 + 3/2], \qquad K' = [3/2\epsilon_2 + 1/2].$$

Since σ is symmetrical in m and n, we can confine ourselves to the case in which

$$\tfrac{1}{2}+\epsilon_1 \leqq \log n/\log m \leqq 1, \tag{2.5}$$

i.e.,

$$m^{\frac{1}{2}+\epsilon_1} \leqq n \leqq m. \tag{2.6}$$

If we write $\epsilon_3 = 4\epsilon_1/3$, we have

$$\nu \leqq \mu \leqq \nu^{\epsilon_3}. \tag{2.7}$$

Hence $T_{K'}(\nu) = O(\nu^2 \log \nu) = o(\mu)$ and we may replace σ by

$$\sigma_1 = 3a/\mu\nu + b/\mu + b/\nu + \{2 - c(\nu/\mu)\}\log(\mu\nu) + D(\nu/\mu) + \nu^{-1}T_K(\mu).$$

3. The integral for $p(m, n)$. We take X, Y small, positive numbers which we define more precisely later. For the present, we require only that

$$X \sim \nu, \qquad Y \sim \mu, \tag{3.1}$$

so that $X = O(Y)$ by (2.7).

We write $x = X + i\theta = X(1 + i\xi)$, $y = Y + i\phi = Y(1 + i\eta)$, where $-\pi \leqq \theta, \phi \leqq \pi$. We write also

$$\lambda^{(1)}(h,k) = \lambda^{(2)}(h,k) = (1 - e^{-hx-ky})^{-1},$$
$$\lambda^{(3)}(h,k) = \lambda^{(4)}(h,k) = 1 + e^{-hx-ky},$$

and

$$f^{(s)}(x,y) = \prod \lambda^{(s)}(h,k),$$

where, for $s = 2$ or 4, h and k each take all positive integral values, while, for $s = 1$ or 3, h and k each take all non-negative integral values, except $h = k = 0$. We see at once that

$$f^{(3)}(x,y) = f^{(1)}(x,y)/f^{(1)}(2x,2y), \quad f^{(4)}(x,y) = f^{(2)}(x,y)/f^{(2)}(2x,2y). \tag{3.2}$$

If we put $p(0,0) = 1$, we verify from the definitions that

$$f(x,y) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} p(m,n)\, e^{-mx-ny}. \tag{3.3}$$

Hence

$$\begin{aligned} p(m,n) &= (1/4\pi^2)\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} f(x,y)\, e^{mx+ny}\, d\theta d\phi \\ &= (XY/4\pi^2)\int_{-\pi/Y}^{\pi/Y}\int_{-\pi/X}^{\pi/X} e^{F(x,y)}\, d\xi d\eta, \end{aligned} \tag{3.4}$$

where

$$F(x,y) = mx + ny + \log f(x,y).$$

We choose ϵ a fixed positive number small enough to ensure that

$$22\epsilon < 1, \qquad 12\epsilon < \epsilon_3 \tag{3.5}$$

and that

$$[\tfrac{1}{2}(1+6\epsilon)(1+1/\epsilon_3)] = [\tfrac{1}{2}(1+1/\epsilon_3)] = [3/8\epsilon_1 + \tfrac{1}{2}] = K-1. \tag{3.6}$$

We write

$$\zeta = (\mu\nu)^{\frac{1}{6}-3\epsilon} = C(mn)^{\epsilon-(1/6)}, \qquad U = \zeta(XY)^{-\frac{1}{2}} \sim C(mn)^{\epsilon}.$$

By a similar argument to that used to prove Lemma 1 of [4], we can prove

LEMMA 1. *If* $\frac{1}{2}\zeta \leqq |\xi| \leqq \pi/X$ *or if* $\frac{1}{2}\zeta \leqq |\eta| \leqq \pi/Y$, *then*

$$|F(x,y)| \leqq F(X,Y) - CU^2.$$

We shall prove later

LEMMA 2. *We can choose* X *and* Y *to satisfy* (3.1) *and such that*

$$F(x,y) - F(X,Y) = -(a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1),$$

whenever

$$|\xi| + |\eta| \leqq \zeta. \tag{3.7}$$

Using these two lemmas, we have from (3.4) that

$$p(m,n) \sim (XYe^{F(X,Y)}/4\pi^2)\{\iint_{|\xi|+|\eta|\leqq\zeta} \exp\{-(a/XY)(\xi^2+\xi\eta+\eta^2)\}\,d\xi d\eta + O(e^{-CU^2}/XY)\}.$$

If we put

$$\xi = (XY)^{\frac{1}{2}}(u+v), \qquad \eta = (XY)^{\frac{1}{2}}(u-v),$$

we have

$$\begin{aligned}\iint_{|\xi|+|\eta|\leqq\zeta} &\exp\{-(a/XY)(\xi^2+\xi\eta+\eta^2)\}\,d\xi d\eta \\ &= 2XY\int_{-U}^{U}\int_{-U}^{U}\exp(-3au^2-av^2)\,dudv \\ &\sim 2XY\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp(-3au^2-av^2)\,dudv = 2\pi XY/3^{\frac{1}{2}}a.\end{aligned}$$

Hence

$$p(m,n) = X^2Y^2e^{F(X,Y)}(3^{\frac{1}{2}}\cdot 2\pi a)^{-1}\{1+o(1)+O(X^{-2}Y^{-2}e^{-CU^2})\} \sim e^{\sigma_2},$$

where

$$\sigma_2 = F(X,Y) + 2\log(\mu\nu) - \log(3^{\frac{1}{2}}\cdot 2\pi a).$$

It remains to prove Lemma 2 and to show that

$$\sigma_2 = \sigma_1 + o(1),$$

that is, that

$$(3.8)\qquad F(X,Y) = 3a/\mu\nu + b/\mu + b/\nu - c(\nu/\mu)\log(\mu\nu) + D(\nu/\mu) + \log(3^{\frac{1}{2}}\cdot 2\pi a) + \nu^{-1}T_K(\mu) + o(1).$$

4. Further results. We use B_k for the k-th Bernoulli number, where

$$u/(e^u-1) = 1 - \tfrac{1}{2}u + \sum_{k=1}^{\infty}(-1)^{k-1}B_ku^{2k}/(2k)! \qquad (|u|<2\pi),$$

and write

$$\gamma_k^{(1)} = \gamma_k^{(2)} = -B_kB_{k+1}/2ka^{(1)}(2k+2)!,$$

$$\gamma_k^{(3)} = \gamma_k^{(4)} = B_kB_{k+1}(2^{2k}-1)/2ka^{(3)}(2k+2)!, \quad (k\geqq 1)$$

$$S_1(x) = 0, \qquad S_H(x) = \sum_{h=1}^{H-1}\gamma_hx^{2h+1} \qquad (H\geqq 2).$$

Henceforth we suppose that (3.7) is satisfied. Then, for any $H\geqq 1$, we can deduce from Theorem 1 of [6] that

$$F(x,y) = mx + ny + a/xy + b/x + b/y - aS_H(x)/y - aS_H(y)/x - c(x/y)\log(xy) + d(x/y) + O(x) + O(y) + O(x^{2H+1}y^{-1}) + O(y^{2H+1}x^{-1}).$$

By (3.1) and (2.7), we have

$$x\sim X\sim \nu, \qquad y\sim Y\sim \mu, \qquad x = O(y) = o(1),$$

and so

$$S_H(x) = O(x^3) = O(y^3) = o(y), \quad x^{2H+1}y^{-1} = O(x^3y^{-1}) = o(1).$$

Hence

$$(4.1)\qquad F(x,y) = mx + ny + a/xy + b/x + b/y - aS_H(y)/x - c(x/y)\log(xy) + d(x/y) + O(y^{2H+1}/x) + o(1).$$

We now introduce the linear operator Ω defined by

$$\Omega g(x,y) = g(x,y) - g(X,Y) - i\xi X(\partial/\partial X)g(X,Y) - i\eta Y(\partial/\partial Y)g(X,Y)$$

where g is any function of the two variables x and y with continuous first derivatives. Trivial calculations show that

$$\Omega(1/xy) = -(\xi^2+\xi\eta+\eta^2)/XY + O(\zeta^3/XY),$$

$$\Omega(1/x) = O(\zeta^2/X), \qquad \Omega(1/y) = O(\zeta^2/Y), \qquad \Omega(x) = \Omega(y) = 0.$$

Now

$$\zeta^3/(XY) = O\{(\mu\nu)^{\frac{1}{2}-9\epsilon}\} = o(1),$$

$$\zeta^2/Y = O(\zeta^2/X) = O(\mu^{1-6\epsilon}\nu^{-6\epsilon}) = O(\nu^{\epsilon_3-6\epsilon\epsilon_3-6\epsilon}) = o(1),$$

since $12\epsilon < \epsilon_3$ by (3.5). Again,

$$\Omega(y^{2h+1}/x) = O(\zeta^2 Y^{2h+1}/X) = o(\zeta^2/X) = o(1) \tag{4.2}$$

when $h \geqq 0$, and

$$\Omega(y\log y/x) = O(\zeta^2 Y\log Y/X) = o(\zeta^2/X) = o(1). \tag{4.3}$$

Hence

$$\Omega(1/xy) = -(\xi^2+\xi\eta+\eta^2)/XY + o(1);$$

and

$$\Omega(1/x), \Omega(1/y), \Omega(x), \Omega(y), \Omega(y^{2h+1}/x), \Omega(x^{-1}y\log y)$$

are all $o(1)$.

We now consider separately the case in which $m^{5/6} \leqq n \leqq m$ and that in which $m^{\frac{1}{2}+\epsilon_1} \leqq n \leqq m^{5/6}$.

5. The case $m^{5/6} \leqq n \leqq m$. In this case we have

$$\log\nu \leqq \log\mu \leqq 4\log\nu/7 + C$$

and so

$$2\log\mu - \log\nu \leqq C + \log\nu/7,$$

$$\begin{aligned} 2\log\zeta - \log\nu &= (1-6\epsilon)\log\mu - 6\epsilon\log\nu \\ &\leqq C + (4/7 - 66\epsilon/7)\log\nu < C + \log\nu/7, \end{aligned}$$

since $22\epsilon < 1$ by (3.5). Hence

$$\mu^2/\nu = O(\nu^{1/7}), \qquad \zeta^2/\nu = O(\nu^{1/7}), \qquad \mu\zeta/\nu = O(\nu^{1/7}). \tag{5.1}$$

From the first of these it follows that $y^3/x \sim \mu^3/\nu = o(1)$. Hence, if we put $H = 1$ in (4.1), we have

$$F(x,y) = F_1(x,y) + F_2(x,y) + o(1), \tag{5.2}$$

where

$$F_1(x,y) = mx + ny + a/xy + b/x + b/y,$$

$$F_2(x,y) = d(x/y) - c(x/y)\log(xy).$$

It follows from the results of the last section that

$$\Omega F_1(x,y) = -(a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1)$$

and so that

$$F_1(x,y) - F_1(X,Y) = i\xi X\partial F_1/\partial X + i\eta Y\partial F_1/\partial Y - (a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1). \tag{5.3}$$

We now choose

$$X = \nu\{1 + ba^{-1}(2\mu - \nu)/3\}, \qquad Y = \mu\{1 + ba^{-1}(2\nu - \mu)/3\}. \tag{5.4}$$

We have

$$X(\partial/\partial X)F_1(X,Y) = mX - a/XY - b/X = (mX^2Y - a - bY)/XY.$$

Since $\nu = O(\mu)$,

$$mX^2Y = m\nu^2\mu\{1 + ba^{-1}(2\mu - \nu)/3\}^2\{1 + ba^{-1}(2\nu - \mu)/3\}$$

$$= a + b\mu + O(\mu^2) = a + bY + O(\mu^2)$$

and

$$\xi X\partial F_1/\partial X = O(\zeta\mu^2/XY) = O(\zeta\mu/\nu) = o(1). \tag{5.5}$$

A similar calculation shows that

$$\eta Y(\partial F_1/\partial Y) = o(1). \tag{5.6}$$

and so (5.3) becomes

$$F_1(x,y) - F_1(X,Y) = -a(\xi^2 + \xi\eta + \eta^2)(XY)^{-1} + o(1). \tag{5.7}$$

The choice of X, Y in (5.4) is, of course, designed to ensure the truth of (5.5) and (5.6), i.e., to take X, Y not at the "saddle-point" but sufficiently near to it.

By (5.4),

$$x/y = X(1+i\xi)/Y(1+i\eta) = (X/Y)\{1+O(\zeta)\} \tag{5.8}$$
$$= (\nu/\mu)\{1+O(\mu)+O(\zeta)\} = (\nu/\mu)+O(\nu)+O(\zeta\nu/\mu).$$

Again,

$$|F_2(x,y)-F_2(\nu,\mu)| \leqq C\mu^2/\nu^2\,|\log(\mu\nu)|\,|x/y-\nu/\mu|+|I(x/y)-I(\nu/\mu)| + o(1).$$

We can show, by the methods of [5], that

$$|I(x/y)-I(\nu/\mu)| \leqq C|x/y-\nu/\mu|\,\mu^2/\nu^2,$$

provided that this is $o(1)$. Now

$$(\mu^2/\nu^2)|x/y-\nu/\mu| = O(\mu^2/\nu)+O(\zeta\mu/\nu) = O(\nu^C)$$

by (5.8) and (5.1). Again, $\log(\mu\nu) = O(\log\nu)$ and so

$$F_2(x,y)-F_2(\nu,\mu) = o(1). \tag{5.9}$$

In the special case $x=X$, $y=Y$, this is

$$F_2(X,Y)-F_2(\nu,\mu) = o(1). \tag{5.10}$$

From (5.2), (5.7), (5.9) and (5.10), we have Lemma 2 for this case. Again, in this case,

$$T_K(\mu) = O(\mu^2\log\mu) = o(\nu)$$

and so, to prove (3.8), it is enough to show that

$$F_1(X,Y)+F_2(X,Y) = 3a/\mu\nu+b/\mu+b/\nu-c(\nu/\mu)\log(\mu\nu) + D(\nu/\mu)+\log(3^{\frac{1}{2}}\cdot 2\pi a)+o(1),$$

that is, in virtue of (5.10) and the definitions of $D(z)$ and $F_1(X,Y)$, that

$$mX+nY+a/XY+b/X+b/Y = 3a/\mu\nu+b/\mu+b/\nu-b^2(\nu/\mu-1+\mu/\nu)/3a+o(1).$$

This follows from (5.4) and the first part of (5.1) with a little calculation.

6. The case $m^{\frac{1}{2}+\epsilon_1} \leqq n \leqq m^{5/6}$. In this case we have

$$x/y \sim X/Y \sim \nu/\mu = n/m = o(1), \qquad x\log y/y = o(1),$$
$$\log y = \log\mu + o(1).$$

Now, by [5], if $|\arg z| < \frac{1}{2}\pi - C$,

$$I(z) = \{(1-\gamma)/12 - \zeta'(-1)\}/z - (\gamma - \log 2\pi)/4 + O(z^3).$$

Hence, if we write $\alpha = b/3a$,

$$\gamma_0 = (12\zeta'(-1) - 1)/12a, \qquad \beta = -1/12a \quad (s = 1, 2),$$

$$\gamma_0 = -\log 2/12a, \quad \beta = 0 \quad (s = 3, 4),$$

$$A^{(1)} = [\log(\mu\nu^2/8\pi^3)]/4, \qquad A^{(2)} = [\log({}^2\pi/\mu)]/4,$$

$$A^{(3)} = -(3\log 2)/4, \qquad A^{(4)} = (\log 2)/4,$$

we have

$$(6.1) \qquad d(\nu/\mu) - c(\nu/\mu)\log(\mu\nu) = A + a\mu\nu^{-1}(\beta\log\mu - \gamma_0) + o(1)$$

and

$$(6.2) \qquad d(x/y) - c(x/y)\log(xy) = A + ayx^{-1}(\beta\log y - \gamma_0) + o(1).$$

Again, by (2.7) and the definitions of K,

$$y^{2K+1}/x \sim \mu^{2K+1}/\nu = O(\nu^{(2K+1)\epsilon_3 - 1}) = o(1).$$

Hence, if we take $H = K$ in (4.1), we have

$$(6.3) \qquad F(x, y) = F_4(x, y) + A + by^{-1} + o(1),$$

where

$$F_4(x, y) = mx + ny + a(xy)^{-1}\chi_K(y),$$

$$\chi_H(y) = 1 + 3\alpha y + y^2(\beta\log y - \gamma_0) - yS_H(y).$$

Now

$$b/y - b/Y = -i\eta/Y(1 + i\eta) = O(\zeta/\mu) = O(\mu^{-\frac{1}{2}-3\epsilon}\nu^{\frac{1}{2}-3\epsilon})$$

$$= O(n^{\frac{1}{2}+\epsilon}m^{-\frac{1}{2}+\epsilon}) = O(m^{(22\epsilon-1)/12}) = o(1),$$

since $n \leqq m^{5/6}$ and $22\epsilon < 1$. Hence

$$F(x, y) - F(X, Y) = F_4(x, y) - F_4(X, Y) + o(1).$$

Now the results of § 4 show that

$$\Omega F_4(x, y) = -a(\xi^2 + \xi\eta + \eta^2)(XY)^{-1} + o(1)$$

and so, to prove Lemma 2, we have only to choose X and Y so that

$$\xi X(\partial F_4/\partial X) = o(1), \qquad \eta Y(\partial F_4/\partial Y) = o(1),$$

that is, so that

$$mX^2Y - a\chi_K(Y) = o(XY/\zeta) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\} \tag{6.4}$$

and

$$nXY^2 - a\omega_K(Y) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}, \tag{6.5}$$

where

$$\omega_H(Y) = \chi_H(Y) - Y\chi'_H(Y) = 1 - Y^2(\beta \log Y + \beta - \gamma_0) + Y^2 S'_H(Y).$$

We write $\delta = \beta \log \mu - \gamma_0$, so that $C < \delta/|\log \mu| < C$ when $s = 1$ or 2, and $\delta = -\gamma_0 = C$ when $s = 3$ or 4.

In the next section we shall prove

LEMMA 3. *For every positive integer h, there exist two polynomials Q_h, R_h of degree $[\frac{1}{2}h]$ in δ whose coefficients depend only on h and s and which have the following property. If*

$$X_H = 1 + \sum_{h=1}^{H-1} R_h \mu^h, \qquad Y_H = 1 + \sum_{h=1}^{H-1} Q_h \mu^h, \tag{6.6}$$

then

$$X_H^2 Y_H = \chi_H(\mu Y_H) + O(\mu^H \delta^{[\frac{1}{2}H]}), \tag{6.7}$$

$$X_H Y_H^2 = \omega_H(\mu Y_H) + O(\mu^H \delta^{[\frac{1}{2}H]}). \tag{6.8}$$

By (3.6)

$$K = [(\tfrac{1}{2} + 3\epsilon)(1 + 1/\epsilon_3)] + 1 > (\tfrac{1}{2} + 3\epsilon)(1 + 1/\epsilon_3) + C$$

and so

$$\epsilon_3(K - \tfrac{1}{2} - 3\epsilon) > \tfrac{1}{2} + 3\epsilon + C.$$

Hence, by (2.7),

$$\mu^{K-\frac{1}{2}-3\epsilon} \leqq \nu^{\epsilon_3(K-\frac{1}{2}-3\epsilon)} < \nu^{\frac{1}{2}+3\epsilon+C}$$

and so

$$\mu^K \delta^{[\frac{1}{2}K]} < (\mu\nu)^{\frac{1}{2}+3\epsilon} \nu^C = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}. \tag{6.9}$$

We now choose $X = \nu X_H$, $Y = \mu Y_H$, so that $X \sim \nu$ and $Y \sim \mu$ as we have supposed. We remark that $m\mu\nu^2 = n\nu\mu^2 = a$. Then, by (6.9) and Lemma 3 with $H = K$, we have

$$m/X^2Y - a\chi_K(Y) = aX_K^2 Y_K - a\chi_K(\mu Y_K) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}$$

and

$$n/XY^2 - a\omega_K(Y) = aX_K Y_K^2 - a\omega_K(\mu Y_K) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}.$$

Hence (6.4) and (6.5) are satisfied and the proof of Lemma 2 is complete.

With these values of X and Y, we have

$$\begin{aligned} F(X,Y) &= F_4(X,Y) + A + (b/Y) + o(1) \\ &= mX + nY + a\chi_K(Y)(XY)^{-1} + A + b/Y + o(1) \\ &= a\Lambda_K/\mu\nu + A + b/\mu - bQ_1 + o(1), \end{aligned}$$

where

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H = 3 + \sum_{h=1}^{2H-1} P_h\mu^h + O(\mu^{2H}\delta^H) \tag{6.10}$$

and P_h is a polynomial of degree $[\frac{1}{2}h]$ in δ. In the next section we shall see how to calculate

$$Q_1 = -\alpha, \qquad P_1 = 3\alpha, \qquad P_2 = \delta - 3\alpha^2.$$

Hence

$$F(X,Y) = 3a/\mu\nu + b/\mu + b/\nu + A + b\alpha + a\mu(\delta - 3\alpha^2)/\nu + \sum_{h=3}^{2K-1} aP_h\mu^{h-1}/\nu + O(\mu^{2K-1}\nu^{-1}\delta^K) + o(1),$$

and (3.8) follows from this and (6.1) and (6.9).

7. Proof of Lemma 3 and calculation of P_h. From (6.7) and (6.8), we obtain

$$Y_H{}^3\chi_H(\mu Y_H) = \{\omega(\mu Y_H)\}^2 + O(\mu^H\delta^{[\frac{1}{2}H]}), \tag{7.1}$$

whence

$$Y_H = 1 + \sum_{h=1}^{H-1} q_h\mu^h Y_H{}^h + O(\mu^H\delta^{[\frac{1}{2}H]}), \tag{7.2}$$

where q_h is a polynomial of degree $[\frac{1}{2}h]$ at most in $\beta\log(\mu Y_H) - \gamma_0 = \delta + \beta\log Y_H$. With sufficient labour, we can solve (7.2) by successive approximations to Y_H of the form

$$Y_H = 1 + Q_1\mu + O(\mu^2\delta), \qquad Y_H = 1 + Q_1\mu + Q_2\mu^2 + O(\mu^3\delta), \ldots$$

and eventually we have

$$Y_H = 1 + \sum_{h=1}^{H-1} Q_h\mu^h.$$

From this and (6.8), we deduce

$$X_H = Y_H{}^{-2}\omega(\mu Y_H) + O(\mu^H\delta^{[\frac{1}{2}H]}) = 1 + \sum_{h=1}^{H-1} R_h\mu^h.$$

Retracing our steps we see that these X_H and Y_H must satisfy (6.7) and (6.8).

We could, of course, add any terms in μ^H and higher powers to X_H and Y_H without affecting the truth of (6.7) and (6.8). Again

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)(X_H Y_H)^{-1}$$

and so

$$\partial\Lambda_H/\partial X_H = 1 - \chi_H(\mu Y_H)/X_H{}^2 Y_H = O(\mu^H \delta^{[\frac{1}{2}H]}) \tag{7.3}$$

by (6.7), and similarly

$$\partial\Lambda_H/\partial Y_H = 1 - \omega_H(\mu Y_H)/X_H Y_H{}^2 = O(\mu^H \delta^{[\frac{1}{2}H]}) \tag{7.4}$$

by (6.8). Hence a change in X_H or Y_H of order $O(\mu^H\delta^{[\frac{1}{2}H]})$ will produce a change of not more than $O(\mu^{2H}\delta^H)$ in Λ_H. Now $X_{H+1} - X_H$ and $Y_{H+1} - Y_H$ are $O(\mu^H\delta^{[\frac{1}{2}H]})$ and $\chi_{H+1}(\mu Y_{H+1}) - \chi_H(\mu Y_{H+1}) = O(\mu^{2H})$. Hence

$$\Lambda_{H+1} - \Lambda_H = O(\mu^{2H}\delta^H)$$

and so in (6.10) the polynomials P_h are independent of H.

We have shown above that Q_h, R_h, P_h exist and can be calculated, but the method of calculation is plainly very laborious. We can, however, shorten the calculations considerably by the following considerations. From (6.7), we have

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H = 2X_H + Y_H + O(\mu^H\delta^{[\frac{1}{2}H]}) \tag{7.5}$$

and so, if we equate coefficients of μ^h, we have

$$2R_h + Q_h = P_h. \tag{7.6}$$

Again,

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H = 3 + \sum_{h=1}^{2H-1} P_h\mu^h + \sum_{h=2H}^{\infty} L_h\mu^h,$$

where L_h is a polynomial in δ of degree $[\frac{1}{2}h]$. This infinite series and its derived series are uniformly and absolutely convergent when $0 < \mu < C$ for some C. Hence

$$\mu(d\Lambda_H/d\mu) = \sum_{h=1}^{2H-1} (hP_h + \beta(dP_h/d\delta))\mu^h + O(\mu^{2H}\delta^H).$$

Now

$$\mu(d\Lambda_H/d\mu) = \mu(\partial\Lambda_H/\partial X_H)(dX_H/d\mu) + \mu(\partial\Lambda_H/\partial Y_H)(dY_H/d\mu) + \mu\chi'_H(\mu Y_H)/X_H.$$

The first two terms on the right are $O(\mu^{H+1}\delta^{[\frac{1}{2}H]})$ by (7.3) and (7.4). Again

$$\chi'_H(\mu Y_H)\mu Y_H = \chi_H(\mu Y_H) - \omega_H(\mu Y_H) = X_H{}^2 Y_H - X_H Y_H{}^2 + O(\mu^H \delta^{[\frac{1}{2}H]})$$

by (6.7) and (6.8). Hence

$$\mu(d\Lambda_H/d\mu) = X_H - Y_H + O(\mu^H \delta^{[\frac{1}{2}H]}).$$

Thus, if we equate "coefficients" of μ^h, we have

$$R_h - Q_h = hP_h + \beta(dP_h/d\delta). \tag{7.7}$$

From (7.6) and (7.7), we have at once

$$Q_h = -(2h-1)P_h/3 - (2\beta/3)(dP_h/d\delta), \tag{7.8}$$

$$R_h = (h+1)P_h/3 + (\beta/3)(dP_h/d\delta).$$

Our method of calculation is now fairly simple. Given Q_h and R_h for $1 \leqq h \leqq H-1$, we use (6.10) to calculate P_h for $H \leqq h \leqq 2H-1$ and (7.8) to calculate Q_h and R_h for $H \leqq h \leqq 2h-1$. We then repeat the process with $2H$ for H. We start with $H=1$, $X_1 = Y_1 = 1$ and can thus calculate P_h for any h. We thus avoid having to solve (7.1) or (7.2), which would be troublesome. The only stage of each cycle which is at all elaborate is the use of (6.10). Using (7.6) in (6.10), we have

$$\chi_H(\mu Y_H)/X_H Y_H = 1 + \sum_{h=1}^{H-1} R_h \mu^h + \sum_{h=H}^{2H-1} P_h \mu^h + O(\mu^{2H}\delta^H).$$

Now

$$\chi_H(\mu Y_H)/Y_H = Y_H{}^{-1} + 3\alpha\mu + \delta\mu^2 Y_H - \sum_{k=1}^{H-2} \gamma_k \mu^{2k+2} Y_H{}^{2k+1} + O(\mu^{2H})$$

$$= 1 + \sum_{h=1}^{2H-1} M_h \mu^h + O(\mu^{2H}\delta^H),$$

where we can calculate the M_h. Finally,

$$1 + \sum_{h=1}^{2H-1} M_h \mu^h = (1 + \sum_{h=1}^{H-1} R_h \mu^h)(1 + \sum_{h=1}^{H-1} R_h \mu^h + \sum_{h=H}^{2H-1} P_h \mu^h) + O(\mu^{2H}\delta^H)$$

and we calculate $P_H, \cdots, P_{2H-1}$ from

$$P_H = M_H - \sum_{h=1}^{H-1} R_h R_{H-h},$$

$$P_{H+1} = M_{H+1} - R_1 P_H - \sum_{h=2}^{H-1} R_h R_{H+1-h},$$

and so on in succession.

If we replace α by $-\alpha$, μ by $-\mu$ but leave δ unchanged (i.e., leave $\log\mu$ unchanged), the sums $\chi_H(\mu Y_H)$ and $\omega_H(\mu Y_H)$ are the same functions of α, μ, δ, Y_H as before. Hence the equation (7.2) is unaltered and so Y_H is unchanged, and so, also, X_H and Λ_H. Hence P_h is an odd or even function of α according as h is odd or even. Since $\alpha^{(2)} = -\alpha^{(1)}$ and $\alpha^{(4)} = -\alpha^{(3)}$, we have

$$P_h^{(2)} = (-1)^h P_h^{(1)}, \qquad P_h^{(4)} = (-1)^h P_h^{(3)}.$$

This remark exactly halves our labour.

We conclude by giving P_h for $h \leqq 7$, first as a polynomial in δ with coefficients in terms of α, β, γ_1, γ_2 and secondly with numerical values.

We have

$$P_0 = 3,\ P_1 = 3\alpha,\ P_2 = \delta - 3\alpha^2,\ P_3 = -3\alpha\delta - \alpha\beta + 7\alpha^3$$

$$P_4 = -\delta^2 + \delta(12\alpha^2 - \beta) - \beta^2/3 + 11\beta\alpha^2/2 - 22\alpha^4 - \gamma_1,$$

$$P_5 = 8\alpha\delta^2 + \delta\alpha(9\beta - 54\alpha^2) + 3\beta^2\alpha - 57\beta\alpha^3/2 + 81\alpha^5 + 5\gamma_1\alpha,$$

$$\begin{aligned} P_6 = {} & 2\delta^3 + \delta^2(23\beta/6 - 55\alpha^2) + \delta(8\beta^2/3 - 66\beta\alpha^2 + 260\alpha^4 + 4\gamma_1) \\ & + 17\beta^3/27 - 133\beta^2\alpha^2/6 + 1787\beta\alpha^4/12 - 988\alpha^6/3 \\ & + 7\beta\gamma_1/3 - 25\gamma_1\alpha^2 - \gamma_2, \end{aligned}$$

$$\begin{aligned} P_7 = {} & -27\alpha\delta^3 + \delta^2\alpha(1078\alpha^2/3 - 319\beta/6) \\ & + \delta\alpha(-112\beta^2/3 + 1351\beta\alpha^2/3 - 1309\alpha^4 - 38\gamma_1) \\ & - 242\beta^3\alpha/27 + 2753\beta^2\alpha^3/18 - 47477\beta\alpha^5/60 + 4301\alpha^7/3 \\ & - 71\beta\gamma_1\alpha/3 + 385\gamma_1\alpha^3/3 + 7\gamma_2\alpha. \end{aligned}$$

If we write

$$P_h^{(1)} = \sum_{k=0}^{[\frac{1}{2}h]} \rho_{hk} (\log\mu)^k,$$

we have the following table for ρ_{hk}.

$h \backslash k$	0	1	2	3
1	.68421639			
2	.05088999	—.06932561		
3	—.04273573	.04743372		
4	.01982883	—.01938670	—.00480604	
5	—.00728059	.00192568	.00876899	
6	.00133717	.00576762	—.00905955	—.00066636
7	.00097131	—.00713373	.00615476	.00205172

For $s=3$, we find that

$P_1 = .45614426$ $P_5 = -.00029313$
$P_2 = -.00528539$ $P_6 = .00001197$
$P_3 = -.00461938$ $P_7 = .00001931$
$P_4 = .00152613$

The following short table of values of $I(n/m)$ was caluculated from the results of [5] by Mr. M. M. Robertson.

$I(0.1) = 2.321694$ $I(0.6) = 0.648918$
$I(0.2) = 1.318405$ $I(0.7) = 0.600774$
$I(0.3) = 0.983921$ $I(0.8) = 0.564468$
$I(0.4) = 0.816592$ $I(0.9) = 0.536012$
$I(0.5) = 0.716076$ $I(1.0) = 0.513011$

UNIVERSITY OF ABERDEEN, SCOTLAND.

REFERENCES.

[1] F. C. Auluck, *Proceedings of the Cambridge Philosophical Society*, vol. 49 (1953), pp. 72-83.

[2] G. Meinardus, *Mathematische Annalen*, vol. 132 (1956), pp. 333-346.

[3] V. S. Nanda, *Proceedings of the Cambridge Philosophical Society*, vol. 53 (1957), pp. 273-277.

[4] E. M. Wright, *Proceedings of the London Mathematical Society*, ser. (3), vol. 7 (1957), pp. 150-160.

[5] ———, *ibid.*, ser. (3), vol. 8 (1958), pp. 312-320.

[6] ———, *Quarterly Journal of Mathematics* (in press).

PRINCIPAL HOMOGENEOUS SPACES OVER ABELIAN VARIETIES.*

By SERGE LANG and JOHN TATE.[1]

Let A be a commutative group variety defined over a field k. If K/k is a Galois extension, the group A_K of points of A rational over K is a module for the Galois group $G(K/k)$, and we denote the associated cohomology groups simply by $H^r(K/k, A)$ or by $H^r(k, A)$ in case K is the separable closure of k. In case K/k is infinite, we mean of course the cohomology groups constructed with cochains of finite type, i.e. coming by inflation from finite extensions.

In § 1, we have carried over to the infinite case the basic propositions of Galois cohomolgy which are familiar in the finite case [2]. This generalization is essentially trivial, but it furnishes a good review for the non-expert, it fixes our notation, and mainly, it is urgently called for when one studies algebraic groups for the following reason: If $A \to B \to C$ is an exact sequence of (separable) homomorphisms defined over k, then $A_K \to B_K \to C_K$ is not necessarily exact but *is* exact if K is the (separable) algebraic closure of k. Actually, in the remainder of the paper, we require the cohomological results only for dimension 1, and most of our applications are based on the special "Kummer sequence" discussed at the end of § 1.

In § 2 we discuss systematically the representation of principal homogeneous spaces for A over k by elements of the 1-dimensional cohomology group (a set if A is non-commutative) $H^1(k, A)$. One establishes an injection of the classes of k-isomorphic spaces into $H^1(k, A)$, and as Serre has remarked, using Weil's theorems concerning the field of definition of a variety, one sees immediately that one actually gets a bijection. Since this representation has been carried out in special cases by F. Chatelet, we call $H^1(k, A)$ the Chatelet group.

Although the rest of the paper is essentially independent of the principal homogeneous space interpretation, it is mainly this interpretation and the consequent relation of the cohomology to diophantine problems which motivates our study of $H^1(k, A)$. For example, as Chatelet has shown, an

* Received January 7, 1958.

[1] Fulbright and Sloan Fellows respectively.

elliptic curve Γ is a homogeneous space over its Jacobian A, and the question whether Γ has a rational point in an extension field K is the same as whether its cohomology class $\alpha(\Gamma) \in H^1(k, A)$ is split by K.

The essential content of this paper is contained in the theorems of the last two sections, which concern the structure of $H^1(k, A)$ when A is an abelian variety.

We first consider the case where k is a local field. After recalling in § 3 some basic facts concerning reduction mod $\mathfrak{p}$, we treat in § 4 the case when A has a non-degenerate reduction. We show (Theorem 1) how the study of elements of order prime to p in $H^1(k, A)$ can be reduced to a study of the reduced variety. There results (Theorem 2) a complete description of the part of $H^1(k, A)$ prime to p when k is a $\mathfrak{p}$-adic number field. In particular, it is a finite group.

In § 5, we deal with global fields, essentially number fields, function fields over algebraically closed fields, or fields of finite type, and obtain various qualitative results. Theorem 3 gives a new variant of the proof that A_k/mA_k is finite. (For another variant, cf. Roquette [10].) From it, we deduce the finiteness of $H^r(K/k, A)$ for finite K/k and all $r > 0$, in Theorem 4. We then consider the subgroup of $H^1(k, A)$ consisting of those elements which split at all primes. Although it is known that this group is not necessarily trivial, we can show that for each integer m (prime to the characteristic of k), its subgroup of elements of period m is finite.

Theorems 6 and 7, which are independent of the preceding five, show on the other hand that $H^1(k, A)$ is large, in different senses. From Theorem 7, it is a corollary that given any positive integer m one can construct a function field in one variable of genus 1, over a suitable algebraic number field k, the degrees of whose divisors rational over k are exactly the multiples of m. One still does not have such examples when $k = \boldsymbol{Q}$ is the field of rational numbers.

1. Galois cohomology. Let k be a field and Ω an algebraically closed field containing k. In Galois cohomology, one deals with a functor A which attaches to each field K between k and Ω a group $A(K)$ and to each k-isomorphism $\phi: K \to K^\phi$, an isomorphism $A(\phi): A(K) \to A(K^\phi)$. The functor is subjected to three axioms:

(A1) For each K we have $A(K) = \bigcup A(F)$, the union being taken over all finitely generated subextensions F/k of K/k.

Notice that (A1) implies that all of our groups $A(K)$ are subgroups

of one big group, namely $A(\Omega)$, and that we have $A(K) \subset A(L)$ whenever $K \subset L$.

(A2) If ψ prolongs ϕ, then $A(\psi)$ prolongs $A(\phi)$. If ψ and ϕ can be composed, then $A(\psi \circ \phi) = A(\psi) \circ A(\phi)$. $A(\text{identity}) = \text{identity}$.

From (A2) it follows that any group of k-automorphisms of a field L operates on $A(L)$.

(A3) If L/K is a Galois extension, then $A(K)$ is the set of fixed points for the operation of the Galois group on $A(L)$.

In most of our applications, A will be (the functor derived from) an algebraic group defined over k, for which $A(K) = A_K$ is the group of points of A which are rational over K, i.e. whose coordinates lie in K, and $A(\phi)$ is the map obtained by applying ϕ to the coordinates.

From now on in this section, we assume that our functor A is commutative, that is, each $A(K)$ is a commutative group. Let K/k be a (possibly infinite) Galois extension. Then $A(K)$ is a module for the Galois group $G(K/k)$, and we can consider the standard r-cochains $a = a(\sigma_1, \cdots, \sigma_r)$ of $G(K/k)$ with values in $A(K)$. We shall say that such a cochain is of *finite type* if there exists a finite sub-extension F such that $a(\sigma_1, \cdots, \sigma_r)$ depends only on the effects of the automorphisms σ_i on F. The cochains of finite type, which are the only ones arising from the usual algebraic processes, form a subcomplex of the standard cochain complex. We shall denote this subcomplex simply by $C(K/k, A)$ and its cohomology groups by $H^r(K/k, A)$. These latter are what we mean by Galois cohomology groups. Of course, if K/k is a finite extension then every cochain is of finite type, and we have achieved nothing but a simplification of notation: $H^r(K/k, A) = H^r(G(K/k), A(K))$. Also, even for infinite K, we have $H^0(K/k, A) = H^0(G(K/k), A(K))$ and this group is just $A(k)$ because of (A3). However, for $r > 0$ and K/k infinite, our groups may differ from the usual ones. For example, if $A(k) = A(K)$, that is, if $G(K/k)$ operates trivially on $A(K)$, then $H^1(K/k, A)$ is the group of continuous homomorphisms of $G(K/k)$ (Krull topology) into $A(K)$ (discrete topology), whereas $H^1(G(K/k), A(K))$ is the group of all homomorphisms.

Let K'/k' be another Galois extension, such that $K' \supset K$ and $k' \supset k$. Then each cochain $a \in C(K/k, A)$ determines a cochain $a' \in C(K'/k', A)$ by the rule $a'(\cdots, \sigma', \cdots) = a(\cdots, \sigma'_K, \cdots)$, where σ'_K denotes the effect on K of $\sigma' \in G(K'/k')$. The cochain map $a \to a'$ induces a homomorphism

$H^r(K/k, A) \to H^r(K'/k', A)$ which we simply call the *canonical* homomorphism. However, in the extreme case $k = k'$, it goes by the name of *inflation* (inf), and in the other extreme case $K = K'$, it is known as *restriction* (res).

PROPOSITION 1. *Let K/k be Galois and let k' be an arbitrary subfield. Then*

$$H^r(K/k', A) = \lim_F \{H^r(F/F \cap k', A)\},$$

the limit being taken inductively with respect to the canonical homomorphisms, as F runs over the finite subextensions of K.

Since passage to (co)homology commutes with inductive limits (cf. [2], Ch. V, Prop. 9.3*), our proposition will follow if we can show that the corresponding formula holds for the cochain groups. Each of the canonical maps $C^r(F/F \cap k', A) \to C^r(K/k', A)$ is an injection, because the inclusion $A(F \cap k') \to A(k')$ is injective and the natural map $G(K/k') \to G(F/F \cap k')$ is surjective. Thus we have only to show that each element $a \in C^r(K/k', A)$ is in the image of $C^r(F/F \cap k', A)$ for some F depending on a. Since a is of finite type, it has only a finite set of distinct values and by Axiom (A1), it follows that we can find a finitely generated, hence finite, sub-extension F/k of K/k such that all valuesof a lie in $A(F)$. Enlarging F, if necessary, so that $a(\sigma_1, \cdots, \sigma_r)$ depends only on the effects of the σ_i on Fk', we can well-define a cochain $b \in C^r(F/F \cap k', A)$ whose image is a by putting $b(\cdots, \sigma_F, \cdots) = a(\cdots, \sigma, \cdots)$, where σ_F denotes the effect of σ on F.

Taking the special case $k' = k$, we find as a corollary

$$H^r(K/k, A) = \lim_F \{H^r(F/k, A)\} = \lim_F \{H^r(G(F/k), A(F))\}.$$

Thus our cohomology groups are just the inductive limits, under inflation, of the ordinary cohomology groups of the finite subextensions.

Let L/K be a Galois extension. A k-isomorphism $\phi: L \to L^\phi$ induces an isomorphism $C(L/K, A) \to C(L^\phi/K^\phi, A)$ by the rule $a^\phi(\cdots, \sigma, \cdots) = \phi a(\cdots, \phi^{-1}\sigma\phi, \cdots)$, and it is a fact that the induced cohomology map $H^r(L/K, A) \to H^r(L^\phi/K^\phi, A)$, called *conjugation*, depends only on the effect of ϕ on K. In particular, if L and K are Galois extensions of k, then the Galois group $G(K/k)$ operates on $H^r(L/K, A)$.

Although there is no doubt that the whole spectral sequence of Hochschild-Serre carries over to the case of infinite Galois extensions we are content here to discuss only a small corner of it, namely:

PROPOSITION 2. *Let $K \supset k'$ be Galois extensions of k. Then there exists*

a canonical transgression homomorphism (tg) *such that the following sequence is exact:*

$$0 \to H^1(k'/k, A) \xrightarrow{\inf} H^1(K/k, A) \xrightarrow{\text{res}} H^1(K/k', A)^{G(k'/k)} \xrightarrow{\text{tg}} H^2(k'/k, A) \xrightarrow{\inf} H^2(K/k, A).$$

Indeed, this proposition is known in the case of ordinary cohomology groups (Cf. Hochschild, G. and Serre, J-P., "Cohomology of Group Extensions," *Trans. A. M. S.*, Vol. 74, 1953). Consequently, for each finite Galois subfield F of K, we have, exactly, with obvious abbreviations of notation:

$$0 \to H^1(F \cap k'/k) \to H^1(F/k) \to H^1(F/F \cap k')^{G(F \cap k'/k)} \xrightarrow{\text{tg}} H^2(F \cap k'/k) \to H^2(F/k).$$

The commutativities required for passing to the inductive limit over F are satisfied and, by Proposition 1, the limit sequence is the one we are looking for. The superscript G on the middle term carries over to the limit because each $(F \cap k'/k)$ is finite.

It is easy to see that our limiting transgression map cap be characterized in the same way as the ordinary one, namely, we have $\alpha = \text{tg}\,\beta$ if and only if there is a cochain $b \in C^1(K/k, A)$ whose restriction to $C^1(K/k', A)$ is a cocycle representing β and whose coboundary δb is the inflation to $C^2(K/k, A)$ of a cocycle $a \in C^2(k'/k, A)$ representing α.

If K/k is Galois and E a finite (not necessarily Galois) subextension, there exists a *transfer* map

$$\text{tr}: H^r(K/E, A) \to H^r(K/k, A)$$

going in the opposite direction from restriction, whose definition we recall here, although we have little use for it in the sequel. Let Φ be the set of $[E: k]$ distinct k-isomorphisms of E. For each $\phi \in \Phi$, let $\phi_* \in G(K/k)$ be a chosen prolongation of ϕ to K. Then for $\sigma \in G(K/k)$, both $\sigma\phi_*$ and $(\sigma\phi)_*$ have the same effect on E, and, consequently, the automorphism $(\sigma\phi)_*^{-1}\sigma\phi_*$, which we shall denote by (σ, ϕ) leaves E elementwise fixed, i.e. belongs to $G(K/E)$. The cohomology transfer is that induced by the cochain transfer $a \to \text{tr}(a)$ defined by

$$(\text{tr}(a))(\sigma_1, \cdots, \sigma_r) = \sum_{\phi \in \Phi} (\sigma_1\sigma_2 \cdots \sigma_r\phi)_* a((\sigma_1, \sigma_2 \cdots \sigma_r\phi), (\sigma_2, \sigma_3 \cdots \sigma_r\phi), \cdots, (\sigma_r, \phi)).$$

Although this cochain transfer depends on the choice of prolongations, the induced cohomology map does not. The main relation between transfer and restriction is the rule $\mathrm{tr} \circ \mathrm{res} = [E: k]$. This and all other such relations can be guessed from the case of dimension 0, where the transfer $A(E) \to A(k)$ is just the *trace*: $a \to \sum \phi a$, and the restriction $A(k) \to A(E)$ is just the inclusion map.

The relation $\mathrm{tr} \circ \mathrm{res} = [E: k]$ shows that if an element $\alpha \in H^r(K/k)$ restricts to 0 in $H^r(K/E)$, then $[E: k]\alpha = 0$. Applying this remark in case $E = K$ is a finite Galois extension of k, we see that $H^r(E/k)$ is a torsion group of exponent $[E: k]$ for $r > 0$, because $H^r(E/E, A) = 0$ for positive r. From Proposition 1, it now follows that the Galois cohomology groups in positive dimension are torsion groups for arbitrary K/k.

We conclude this section by considering the cohomology maps induced by a *homomorphism* $f: A \to B$ of one of our functors into another. By this we mean a collection of homomorphisms $f(K): A(K) \to B(K)$ satisfying

(f1) If $L \supset K$, then $f(K)$ is the restriction of $f(L)$ to $A(K)$.

(f2) If $\phi: K \to K^\phi$ is a k-isomorphism, then

$$f(K^\phi) \circ A(\phi) = B(\phi) \circ f(K).$$

For example, suppose A and B are algebraic groups defined over k. Then a k-homomorphism $f: A \to B$ (that is, an everywhere defined rational map over k which is a group homomorphism) yields a homomorphism of the functor A into the functor B. We simply let $f(K)$ denote the restriction of f to $A(K)$. Condition (f2) is satisfied because f is defined over k.

A functor homomorphism $f: A \to B$ gives rise to cohomology homomorphisms

$$H^r(K/k, A) \to H^r(K/k, B),$$

namely, those induced by the cochain map $a \to f \circ a$, and these induced cohomology maps obviously commute with canonical maps, conjugations, and transfers. A sequence of functor homomorphisms $A' \to A \to A''$ is said to be *K-exact* if the sequence $A'(K) \to A(K) \to A''(K)$ is exact in the ordinary sense.

PROPOSITION 3. *Let K/k be Galois. A K-exact sequence*

$$0 \to A' \to A \to A'' \to 0$$

gives rise to an infinite exact cohomology sequence

$$\cdots \to H^r(K/k, A) \to H^r(K/k, A'') \xrightarrow{\delta} H^{r+1}(K/k, A') \to H^{r+1}(K/k, A) \to \cdots.$$

This proposition follows as usual from the lemma: *If* $A' \to A \to A''$ *is* K*-exact, then the cochain sequence*

$$C(K/k, A') \to C(K/k, A) \to C(K/k, A'')$$

is exact. If a cochain $a \in C(K/k, A)$ goes to 0 in $C(K/k, A'')$, then each of its values goes to 0 in $A''(K)$. Hence, by K-exactness, we can pick a pre-image in $A'(K)$ for each of these values and thereby define a cochain a' whose image is a. Moreover, a' will be of finite type, provided we select one single pre-image for each of the distinct values of a, because of Axiom (A1).

In many applications, we shall deal with the case where K is the separable closure k_s of k, and where the sequence of Proposition 3 is k_s-exact. The resulting cohomology sequence involves the cohomology groups $H^r(k_s/k, A)$ which we shall simply write $H^r(k, A)$ since they occur so frequently.

Such a sequence arises from commutative algebraic groups. As a matter of notation, if X is an abelian group and m a natural number, we shall denote by X_m the kernel of the map $X \xrightarrow{m} X$. Let A be a commutative group variety defined over k. If m is prime to the characteristic, the sequence

$$0 \to A_m \to A \xrightarrow{m} A \to 0$$

is k_s-exact. Writing A_K instead of $A(K)$, our cohomology sequence becomes

$$0 \to A_m \cap A_k \to A_k \xrightarrow{m} A_k \to H^1(k, A_m) \to H^1(k, A) \xrightarrow{m} H^1(k, A) \to \cdots.$$

A portion of this exact sequence may be written more simply as follows.

$$0 \to A_k/mA_k \to H^1(k, A_m) \to H^1(k, A)_m \to 0.$$

The group A_k/mA_k is well known to be of interest in arithmetical questions, and we shall investigate it from this point of view in § 5. For the moment, we assume further that $A_m \subset A_k$, and let G_k be the Galois group of k_s over k, i.e. $G_k = G(k_s/k)$. Then G_k operates trivially on A_m, and our sequence becomes

$$0 \to A_k/mA_k \to \mathrm{Hom}(G_k, A_m) \to H^1(k, A)_m \to 0,$$

where Hom means, of course, the continuous homomorphisms as always. We shall have many applications for this sequence, and we shall call it the *Kummer* sequence, because, in case A is the multiplicative group, we have

$H^1(k, A) = 0$ by Hilbert's Theorem 90, so that we find the familiar Kummer duality

$$k^*/k^{*m} \approx \mathrm{Hom}(G_k, A_m),$$

always provided that the group of m-th roots of unity A_m is contained in $A_k = k^*$.

2. Principal homogeneous spaces. Let A be a functor of the type described in the first paragraph of § 1. If the groups $A(K)$ are not commutative, we cannot define cohomology groups $H^r(K/k, A)$ for Galois extensions K/k. The best we can do is define cohomology *sets* in dimension *one*, as follows. We consider 1-cochains a of finite type and we call 1-cocycles those satisfying the identity $a_\sigma a_\tau{}^\sigma = a_{\sigma\tau}$. Here we write $A(K)$ multiplicatively and write a_σ instead of $a(\sigma)$ for $\sigma \in G(K/k)$. We do not attempt to multiply 1-cocycles, but we explain when two 1-cocycles a and a' are cohomologous, namely, when there exists an element $b \in A(K)$ such that $a'_\sigma = b^{-1} a_\sigma b^\sigma$. The cohomology thus defined is an equivalence relation, and we denote the set of equivalence classes by $H^1(K/k, A)$. This set is not a group but it does have a distinguished element, namely the class of coboundaries of the form $a_\sigma = b^{-1} b^\sigma$, which we call the trivial class.

The reader will easily verify that the canonical maps, in particular, restriction and inflation, the conjugation maps, and the induced maps make sense for this non-commutative cohomology.

Proposition 1 holds in dimension 1.

Proposition 2 holds in a weaker form, namely, in the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\inf} H^1(K/k, A) \xrightarrow{\mathrm{res}} H^1(K/k', A)^{G(k'/k)}$$

inf is an injection whose image is the inverse image of the trivial class under restriction.

Proposition 3 collapses to the exactness of the sequence

$$0 \to A(k) \to B(k) \to C(k) \xrightarrow{\delta} H^1(K/k, A) \to H^1(K/k, B) \to H^1(K/k, C),$$

where we now deal with a K-exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

Here exactness means that the image of each map is the inverse image of the

trivial element under the succeeding map, and there is the additional feature that δ injects the right coset space $C(k)/gB(k)$ into $H^1(K/k, A)$.

Suppose now that A is a group variety defined over k. We wish to explain the connection between the 1-dimensional cohomology sets and the right principal homogeneous spaces for A. To recall the definition of this latter object, a right phs for A over k is a variety V defined over k on which A operates simply and transitively, in such a way that the map $(v, w) \to v^{-1}w$ of $V \times V$ into A is an everywhere defined rational map over k. Here we use the symbol $v^{-1}w$ to denote the uniquely determined element of A which carries the point v into the point w, so that the formula $v(v^{-1}w) = w$ becomes an identity. Two phs's V and V' are said to be *k-isomorphic* if there exists a birational biholomorphic transformation $f: V \to V'$ such that $f(va) = f(v)a$ for $v \in V$ and $a \in A$. Among the k-isomorphism classes, there is a distinguished class, namely, the class of spaces which are k-isomorphic to A itself, viewed as phs under right multiplication. A space is in this class if and only if it has a rational point in k. In case A is commutative, Weil [13] has defined a geometric law of composition which makes the classes of phs's into a commutative group.

The following proposition has been proved by F. Chatelet [3], [4] for various special groups.

PROPOSITION 4. *Let K/k be a Galois extension. There is a canonical bijection between the first cohomology set $H^1(K/k, A)$ and the set of k-isomorphism classes of principal homogeneous spaces for A over k which have rational points in K. This bijection is a group isomorphism when A is commutative.*

Proof. Let V be a phs with a rational point v in K. Each such point gives rise to a 1-cocycle $a_\sigma = v^{-1}v^\sigma$. The different choices of v lead to cocycles filling out a cohomology class. Denote this class by $\alpha(V)$. If V and V' are k-isomorphic, then points v and v' which correspond under a k-isomorphism yield the same cocycle; hence $\alpha(V) = \alpha(V')$. Conversely, if V and V' are given such that $\alpha(V) = \alpha(V')$, then there do exist points v and v' yielding the same cocycle. When this is the case, the map $x \to v'(v^{-1}x)$ is a k-isomorphism of V onto V'. Indeed, it is a K-isomorphism, and a simple computation shows that it is invariant under all $\sigma \in G(K/k)$. We have thus obtained an injection of the classes of spaces into the cohomology set.

As Serre has observed, it follows immediately from Weil's theorems concerning the field of definition of a variety that every cocycle comes from a

space. Indeed, consider the transformations $f_\sigma : A \to A$ defined by $f_\sigma(x) = a_\sigma x$. They satisfy the identity $f_\sigma \circ f_\tau^\sigma = f_{\sigma\tau}$. Since the cocycle a is of finite type, it follows from [14] that there exists a variety V defined over k and a birational biholomorphic transformation $F : A \to V$ defined over K such that $f_\sigma = F^{-1} \circ F^\sigma$. The operation $vb = F(F^{-1}(v)b)$ for $v \in V$ and $b \in A$ makes V into a phs for A over k, not only over K, because a simple computation shows that $(v^{-1}w)^\sigma = ((v^\sigma)^{-1}w^\sigma)$. Finally, one sees that the cocycle a with which we started is that arising from the point $v = F(1)$ on V.

If A is commutative, let U, V, W be phs's and suppose $f : U \times V \to W$ is an everywhere defined rational map over k which exhibits the fact that the class of W is the product of the classes of U and V (cf. [13], prop. 5). Select $u \in U$, $v \in V$ rational over K and put $w = f(u, v)$. Using the characteristic property of f, namely $f(ua, vb) = f(u, v)ab$, one finds that the cocycle derived from w is the product of those derived from u and v. This concludes the proof.

Since every variety defined over k has a point whose coordinates lie in the separable algebraic closure k_s of k, it follows from Proposition 4 that the set (group) of all principal homogeneous spaces for A over k is isomorphic to $H^1(k_s/k, A)$ which we have agreed to write $H^1(k, A)$, and which we shall call the *Chatelet set* (*group*) for A over k.

If k' is an extension field of k, it is obvious that the canonical cohomology map $H^1(k, A) \to H^1(k', A)$ reflects the homogeneous space operation of extending the ground field from k to k'. The cohomology classes in the kernel of this map are said to be *split* by k', and the same terminology is applied to the corresponding homogeneous spaces. Thus a phs for A over k is *split* by an extension k' if and only if it is k'-isomorphic to A, or what is the same, if and only if it has a rational point in k'. In case k'/k is a Galois extension, the exactness of the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(k, A) \xrightarrow{\text{res}} H^1(k', A)$$

is obvious from the point of view of homogeneous spaces, for the cohomology inflation map simply reflects the inclusion of the set of phs's split by k' in the set of all phs's for A over k.

Let X be a variety defined over k. We define the *index* of X over k ($\operatorname{ind} X$) to be the greatest common divisor of the degrees of the 0-cycles on X which are prime rational over k. The degree of a prime rational 0-cycle is equal to the degree of the extension generated over k by the coordinates of one of its points. Thus, in the case of a principal homogeneous space V

for A over k, we see that $\operatorname{ind} V$ is the greatest common divisor of the degrees of the finite extensions of k which split V, and is consequently subject to a cohomological analysis.

From now on, we assume that A is commutative. Defining the *separable index* of V ($\operatorname{ind}_s V$) as the greatest common divisor of the degrees of the finite separable splitting extensions, and the *period* of V ($\operatorname{per} V$) as the period of V in the group of classes of principal homogeneous spaces for A over k, we have

PROPOSITION 5. *Let V be a principal homogeneous space for A over k. Then* $\operatorname{per} V$ *divides* $\operatorname{ind} V$ *divides* $\operatorname{ind}_s V$, *and all three numbers have the same prime factors.*

Proof. It is trivial that the index divides the separable index. Let v_0 be a rational point of V in some Galois extension of k. Let $f: V \to A$ be the map $v \to v_0^{-1} v$, and let $a_\sigma = v_0^{-1} v^\sigma$ be the cocycle determined by v_0. Then for any point $v \in V$, we have $a_\sigma (f(v))^\sigma = f(v^\sigma)$, and consequently, by linearity, we have

$$a_\sigma^{\deg(\mathfrak{v})} (f(\mathfrak{v}))^\sigma = f(\mathfrak{v}^\sigma)$$

for any 0-cycle $\mathfrak{v}$ on V. If $\mathfrak{v}$ is rational over k and of degree d, then $\mathfrak{v}^\sigma = \mathfrak{v}$, and the d-th power of the cocycle a_σ is split by the coboundary of $f(\mathfrak{v})$. This proves that the period divides the index.

Finally, let p be a prime number not dividing the period. We must show that p does not divide the separable index, that is, we must construct a finite separable splitting extension E_p whose degree is not divisible by p. To this effect, we simply take any finite Galois splitting extension K/k and let E_p be the subextension cut out by a p-Sylow subgroup of $G(K/k)$. If $\alpha \in H^1(K/k, A)$ is the cohomology class of V, then the period of $\operatorname{res} \alpha \in H^1(K/E, A)$ divides the p-power $[K : E]$ on the one hand, and divides $\operatorname{per} V$ on the other. Consequently, $\operatorname{res} \alpha = 0$, i.e. E splits V.

The reader will have noticed the analogy between the Chatelet group of classes of principal homogeneous spaces for A over k and Brauer's group of classes of central simple algebras over k. We have in fact taken over Proposition 5 and its proof almost word for word from the theory of algebras. In the case of algebras, the period is not in general equal to the index as a counterexample of Albert [1] shows. We have found a similar counterexample in the case of principal homogeneous spaces (end of § 4). Nevertheless, our counterexample, like Albert's, involves a comparatively

complicated ground field k, and over number fields and their completions, all examples which we have satisfy the condition period = index.

The theory of algebras suggests other questions. Since every central division algebra contains a separable splitting field, it is true for algebras that (1) the index equals the separable index, and (2) the index is not only the greatest common divisor, but is actually the minimum of the degrees of the finite splitting fields. We have not investigated the corresponding statements for homogeneous spaces, except to notice that (2) is true in case A is an elliptic curve, for in that case, the Riemann-Roch theorem shows that every divisor class of positive degree contains positive diivsors.

The divisibilities of Proposition 5 imply

COROLLARY. *Suppose $\alpha \in H^1(k, A)$ is of period m and is split by an extension E/k of degree m. Then the corresponding homogeneous space has index m.*

This corollary will enable us to construct, with abelian varieties A, over various ground fields k, examples of spaces whose index is a preassigned integer m (cf. Theorem 7, § 5). These examples are of particular interest in case A is an elliptic curve. Then V, which becomes birationally equivalent to A over an extended ground field, is also a curve of genus 1. The point is that the index of a curve of genus $g \neq 1$ is bounded by, and in fact divides, $2g-2$, for the Riemann-Roch theorem shows the existence of divisors rational over k of degree $2g-2$. On the other hand, our examples show that the index is completely arbitrary for $g = 1$, a fact conjectured by Artin, but unknown until now.

3. Non-degenerate reduction. Throughout this section, we assume that we have a field k and a place of k onto a field k' such that any two extensions of it to the algebraic closure $\bar{k}$ of k are conjugate over k'. In terms of valuations, this means that the extension of the valuation is unique, and this condition is certainly satisfied if k is complete, and the valuation discrete.

We denote by θ a definite extension of our place to $\bar{k}$. An automorphism σ of $G(\bar{k}/k)$ induces an automorphism σ' of the algebraic closure of k', characterized by the relation $\theta\sigma = \sigma'\theta$. The map $\sigma \to \sigma'$ is a homomorphism of $G(\bar{k}/k)$ onto $G(\bar{k}'/k')$.

We shall also assume that the valuation is discrete, although this can presumably be dispensed with. If Z is a cycle rational over an algebraic extension K of k (say in some projective space), then it has a reduction, or, as we shall also say, a specialization Z' in the reduced projective space determined by θ, and rational over K' (Shimura [12]). The only facts concerning

the specialization $Z \to Z'$ which we shall use in the sequel is that it commutes with projections and intersections, i.e. under suitable hypotheses, $(\mathrm{pr}\, Z)' = \mathrm{pr}(Z')$, and for two positive cycles X, Y, we have $(X \cdot Y)' = X' \cdot Y'$. We refer to [12] for the proof.

Our place θ induces a mapping of points P of our projective space, algebraic over k, onto points P', algebraic over k'. We shall also write $P' = \theta P$. We have for any automorphism σ of $\bar{k}/k$, $(\sigma P)' = \sigma' P'$. If Z is a positive cycle, then $\mathrm{supp}(Z') = (\mathrm{supp}\, Z)'$.

We shall now list a few properties of reduction of cycles, and especially varieties in non-degenerate cases.

To begin with, we have a result which will serve as Hensel's lemma for points on varieties.

LEMMA. *Let $\mathfrak{a}$ be a positive 0-cycle rational over k. Let P' be a point of $\mathfrak{a}'$ which occurs in $\mathfrak{a}'$ with multiplicity* 1. *Then there exists a unique point P of $\mathfrak{a}$ specializing to P', and P is rational over k.*

Proof. Note that P' is rational over k' since $\mathfrak{a}'$ is rational over k'. Let P be in $\mathfrak{a}$, specializing to P'. Then obviously P occurs with multiplicity 1, so that P is separable over k. If σ is any automorphism of $\bar{k}$ over k, then $(\sigma P)' = (\sigma' P') = P'$, and hence σP also specializes to P'. Since $\mathfrak{a}$ is rational over k, it follows that σP also occurs in $\mathfrak{a}$, and since P' has multiplicity 1, we conclude that $\sigma P = P$, and hence that P is rational over k.

We now have the surjectivity of θ, whose proof is due to Chow.

PROPOSITION 6. *Let the cycle Z be a variety V, and assume that Z' is also a variety V', i.e. consists of one component with multiplicity* 1. *Let P' be a simple point of V', rational over k'. Then there exists a point P of V rational over k which specializes to P'.*

Proof. Our statement being local, we may assume that V' is affine. There exists a linear variety L' defined over k' such that $V' \cdot L'$ is defined and contains P' with multiplicity 1. Lift L' to a linear variety L over k, such that $V \cdot L$ is defined. Then $V \cdot L$ contains a point P specializing to P'. Since $V \cdot L$ is rational over k, we need merely apply the lemma and the compatibility of specializations with intersections to conclude the proof.

For the applications, we are principally interested in abelian varieties. Let A be an abelian variety defined over k. Its specialization A' is then a cycle. If this cycle has one component with multiplicity 1, which is an abelian variety whose law of composition is obtained by reduction of that of A, then we shall say that the specialization $A \to A'$ is *non-degenerate*. (The uniqueness of non-degenerate specializations has been proved in [5].) In that case, if a, b are two points of A algebraic over k, then $(a + b)' = a' + b'$,

the first $+$ referring to addition on A and the second on A'. In view of Proposition 6, we have an exact sequence

$$0 \to S_k \to A_k \to A'_{k'} \to 0,$$

where S_k is simply the kernel of the specialization homomorphism θ. If K is a finite Galois extension of k with group G then each one of the groups S_K, A_K, $A'_{K'}$ is a G-module, in view of the relation $(\sigma x)' = \sigma' x'$. It is to the exact sequence

$$0 \to S_K \to A_K \to A'_{K'} \to 0$$

that we shall apply the cohomology theory in the next section.

Suppose for a moment that k is a p-adic field $\boldsymbol{Q}_p$ and A is an elliptic curve of the type considered by Lutz [8]. Then A_k contains a subgroup isomorphic to the integers of $\boldsymbol{Q}_p$, which is none other than our kernel S_k when A' is non-degenerate. More generally, if k is an arbitrary $\mathfrak{p}$-adic field, and A an abelian variety of dimension r, then Mattuck [9] has shown that A_k contains a subgroup isomorphic to r copies of the integers of k. We can always choose such a subgroup M_k of Lutz-Mattuck such that $M_k \subset S_k$. We shall prove below that S_k is uniquely divisible by an integer m prime to p. From this one sees that $(S_k : M_k)$ is a power of p.

We return to an arbitrary field k subject to the conditions stated at the beginning of this section. Let m be an integer not divisible by the characteristic p of k'. Let a be a point of A rational over k. The cycle

$$(m\delta)^{-1}(a) = \mathrm{pr}_1\{\Gamma \cdot (A \times (a))\},$$

where Γ is the graph of $m\delta$, consists of the points x on A such that $mx = a$, each one occurring with multiplicity 1. Specializing, we see that

$$[(m\delta)^{-1}(a)]' = (m\delta')^{-1}(a'),$$

where δ' is the identity on A'. Taking $a = 0$, this shows in particular that θ induces an isomorphism of the points of finite order prime to p on A onto those points on A', i.e. of A_m onto A'_m. Actually, from Hensel's lemma, we get

PROPOSITION 7. *Assume that the specialization $A \to A'$ is non-degenerate. Let m be an integer prime to p. Then the homomorphism θ induces an isomorphism of $A_m \cap A_k$ onto $A'_m \cap A'_{k'}$.*

Furthermore, we also get information concerning the kernel S_k in our exact sequence above.

PROPOSITION 8. *Assume that the specialization $A \to A'$ is non-degenerate. Let m be an integer prime to p. Then S_k is uniquely divisible by m.*

Proof. Let a be in S_k, so that $a' = 0'$. The cycle $(m\delta)^{-1}(a)$ specializes to the cycle $(m\delta')^{-1}(a') = (m\delta')^{-1}(0')$ which consists of the points of order m on A'. Since $(0')$ occurs with multiplicity 1 in the reduced cycle, it follows by Hensel's lemma that there is exactly one point on $(m\delta)^{-1}(a)$ which specializes to $0'$ and that this point is rational over k.

PROPOSITION 9. *Assume that the specialization $A \to A'$ is non-degenerate. Let m be an integer prime to p. Let a be a point of A_k, and let $K = k(1/m \cdot a)$ be the field obtained by adjoining all points x such that $mx = a$. Then K is unramified over k, and $K' = k'(1/m \cdot a')$.*

Proof. This is again an immediate consequence of Hensel's lemma. Taking into account the fact that the points in $(m\delta')^{-1}(a')$ are all separable over k', we see that K is in fact the uniquely determined unramified extension of k such that $K' = k'(1/m \cdot a')$.

We conclude this section by a remark on the reduction of principal homogeneous spaces. Let V be such a space over A, defined over k. Suppose that V' has one component with multiplicity 1. Then V' has a simple rational point in some separable extension of k', and hence, by Proposition 6, V has a point in, and is split by, an unramified extension of k.

4. Cohomology and non-degenerate reduction. Let k be a field complete with respect to a discrete valuation and let A be an abelian variety defined over k which has a non-degenerate reduction A' modulo the prime in k. The only fields we consider are the algebraic extensions K of k and their residue class fields K'. From the preceding section we know the following facts:

(R1) The reduction map $\theta_K : A_K \to A'_{K'}$ is surjective for each K and its kernel S_K is uniquely divisible by an integer m prime to the residue class characteristic, p.

(R2) If K' is separably closed, then $A'_{K'}$ is divisible by m and contains A'_m for m prime to p.

The following cohomological analysis makes no reference to the details of the reduction process itself, nor even to abelian varieties. It applies to any pair of commutative functors A and A' of the fields K and K' (in the sense of § 1) which are linked by a natural homomorphism $\theta : A \to A'$ so that conditions (R1) and (R2) are satisfied. Note that (R1) implies, trivially,

(R1′) θ_K induces a bijection $A_m \cap A_K \to A'_m \cap A'_{K'}$ for each K, and m prime to p.

Let k_u denote the maximal unramified extension of k. Then the residue class field of k_u is the separable closure of the residue class field of k, or in symbols, $(k_u)' = (k')_s$.

For the rest of this section, we let m be an integer prime to p. Our goal is now Theorem 1 below.

LEMMA 1. *If $K \supset k_u$, then A_K is divisible by m and contains A_m.*

Proof. K' is separably closed because $K \supset k_u$. Hence, by (R2), we know the divisibility by m of the factor group $A_K/S_K \approx A'_{K'}$. Since from (R1), we know S_K is also divisible by m, we conclude that A_K is. We also know from (R2) that $A'_m \subset A'_{K'}$. This together with (R1') implies that $A_m \cap A_K$ is independent of K for $K \supset k_u$, and consequently, $A_m \subset A_K$.

The group Ω_m of m-th roots of unity is contained in k_u, and the group of units in k_u is divisible by m. Therefore the maximal abelian extension of k_u of exponent m is the field $k_u(\pi^{1/m})$ obtained by adjoining the m-th root of any prime element π of k_u. The Galois group of this extension is canonically isomorphic to Ω_m. Indeed, the map $\sigma \to \zeta_\sigma = (\pi^{1/m})^{\sigma-1}$ is a homomorphism of G_{k_u} onto Ω_m, whose kernel cuts out $k_u(\pi^{1/m})$, and this homomorphism is independent of π and its chosen m-th root.

LEMMA 2. *There is a canonical isomorphism*

$$\mathrm{Hom}(\Omega_m, A_m) \approx H^1(k_u, A)_m$$

which attaches to each homomorphism $\chi: \Omega_m \to A_m$ the cohomology class of the cocycle $\sigma \to \chi(\zeta_\sigma)$, $\sigma \in G(k_s/k_u)$.

Proof. Since A_{k_s} is divisible by m, the Kummer sequence at the end of § 1 is applicable, and since A_{k_u} is divisible by m, it yields an isomorphism

$$\mathrm{Hom}(G_{k_u}, A_m) \approx H^1(k_u, A)_m.$$

Since A_m is commutative of exponent m, any homomorphism $h: G_{k_u} \to A_m$ will have the property that $h(\sigma)$ depends only on the effect of σ on an abelian extension of exponent m. Consequently, according to the discussion preceding this lemma, we can factor h through $\sigma \to \zeta_\sigma$, i.e. we can write $h(\sigma) = \chi(\zeta_\sigma)$ for some $\chi: \Omega_m \to A_m$.

The Galois group G_k of k_s/k operates on $H^1(k_u, A)$ as explained in § 1. It also operates on Ω_m and on A_m, and consequently, on $\mathrm{Hom}(\Omega_m, A_m)$ in the usual manner, so that

$$(\chi^\phi)(\zeta^\phi) = \phi(\chi(\zeta))$$

for $\phi \in G_k$.

LEMMA 3. *The isomorphism of Lemma 2 is a G_k-isomorphism.*

Proof. Let $\chi \in \mathrm{Hom}(\Omega_m, A_m)$ and let $a_\sigma = \chi(\zeta_\sigma)$ be the corresponding cocycle. Let $\phi \in G_k$. Then for $\sigma \in G_{k_u}$, we have

$$(a^\phi)_\sigma = \phi a_{\phi^{-1}\sigma\phi} = \phi\chi(\zeta_{\phi^{-1}\sigma\phi}) = \chi^\phi(\zeta_{\phi^{-1}\sigma\phi^\phi}) = \chi^\phi(\zeta_\sigma)$$

because

$$\zeta_{\phi^{-1}\sigma\phi^\phi} = (\pi^{1/m})^{\sigma\phi-\phi} = ((\pi^\phi)^{1/m})^{\sigma-1} = \zeta_\sigma.$$

Note that because of the way G_k is defined to operate on $\mathrm{Hom}(\Omega_m, A_m)$, we have

$$\mathrm{Hom}(\Omega_m, A_m)^{G_k} = \mathrm{Hom}_{G_k}(\Omega_m, A_m);$$

in other words, a homomorphism is left fixed by the operation of G_k if and only if it is a G_k-isomorphism.

LEMMA 4. *The sequence*

$$0 \to H^1(k_u/k, A)_m \xrightarrow{\inf} H^1(k, A)_m \xrightarrow{\mathrm{res}} [H^1(k_u, A)_m]^{G_k} \to 0$$

is exact.

Proof. Of course, it is only necessary to prove that the restriction is surjective. By the preceding lemmas, an element $\alpha \in H^1(k_u, A)_m$ which is invariant under G_k will be represented by a cocycle of the form $a_\sigma = \chi((\pi^{1/m})^{\sigma-1})$, $\sigma \in G_{k_u}$, where $\chi: \Omega_m \to A_m$ is a G_k-homomorphism. Here π is an arbitrary prime in k_u. Choosing π in k, and choosing a definite m-th root, we see that that the expression for a_σ makes sense for all $\sigma \in G_k$, not only for $\sigma \in G_{k_u}$. Now

$$\sigma \to (\pi^{1/m})^{\sigma-1}$$

is a cocycle in Ω_m (it is a coboundary in Ω), and since $\chi: \Omega_m \to A_m$ is a G_k-homomorphism, it follows that a_σ is still a cocycle. By construction, its class $\beta \in H^1(k, A)_m$ restricts to α.

Since k_u/k is unramified, its Galois group may be identified with the Galois group of its residue class extension. We shall make this identification from now on, and will designate both groups by the simpler symbol $G_{k'}$. Of course, $\theta: A_{k_u} \to A'_{k'_u}$ is a $G_{k'}$-homomorphism.

LEMMA 5. *θ induces an isomorphism $H^1(k_u/k, A)_m \approx H^1(k', A')_m$.*

Proof. Since A_{k_u} and $A'_{k'_u}$ are divisible by m, we can apply the Kummer sequence to the extensions k_u/k and k'_u/k', obtaining the exact horizontal rows in the diagram

$$\begin{array}{ccccccc}
0 \to & A_k/mA_k & \to H^1(k_u/k, A_m) & \to H^1(k_u/k, A)_m & \to 0 \\
& \downarrow \theta & \downarrow \theta & \downarrow \theta & \\
0 \to & A'_{k'}/mA'_{k'} & \to H^1(k', A'_m) & \to H^1(k', A')_m & \to 0
\end{array}$$

The left vertical arrow is surjective by (R1). The middle is bijective because A_m is $G_{k'}$-isomorphic to A'_m (recall that $G_k = G(k_u/k)$). Consequently, the right vertical arrow is bijective as contended.

Putting our results together, we see that we have proved a good part of

THEOREM 1. *Let k be a field complete with respect to a discrete valuation with residue class field k' of characteristic $p \geqq 0$. Let A and A' be two commutative functors as in § 1, satisfying* (R1) *and* (R2). *Then for each natural number m not divisible by p, there exists a canonical exact sequence*

$$0 \to H^1(k', A')_m \to H^1(k, A)_m \to \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m) \to 0,$$

where Ω'_m is the group of m-th roots of unity in the residue field. Furthermore, if K is a finite extension of k with ramification index e, the following diagram is commutative:

$$\begin{array}{ccccc} H^1(k', A')_m & \to & H^1(k, A)_m & \to & \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m) \\ \Big\downarrow \mathrm{res} & & \Big\downarrow \mathrm{res} & & \Big\downarrow e \\ H^1(K', A')_m & \to & H^1(K, A)_m & \to & \mathrm{Hom}_{G_K}(\Omega'_m, A'_m). \end{array}$$

Proof. The indicated exact sequence results from the preceding two lemmas and the trivial replacement of Ω_m and A_m by the isomorphic Ω'_m and A'_m. The commutativity of the left square is obvious. That of the right follows from the relationship

$$\chi((\pi^{1/m})^{\sigma-1}) = \chi^e((\pi_1^{1/m})^{\sigma-1})$$

for $\sigma \in G_{K_u}$, where π_1 is a prime in K_u and $\pi \sim \pi_1^e$ is a prime in k_u.

Naturally, we are interested here in the case where the functors are given by an abelian variety A defined over k, and a non-degenerate reduction A'. Theorem 1 gives especially precise information when $H^1(k', A') = 0$. This is the case, for example, if k' is algebraically closed, or finite [7]. Then we obtain simply an isomorphism

$$H^1(k, A)_m \approx \mathrm{Hom}_{G_{k'}}(\Omega'_m, A'_m).$$

From the commutative diagram of the theorem, we obtain the following corollaries.

COROLLARY 1. *Assume k' is either finite or algebraically closed. Let A be an abelian variety defined over k, with a non-degenerate reduction A'. Then a finite extension K/k splits an element $\alpha \in H^1(k, A)_m$ if and only if the ramification index $e(K/k)$ is divisible by the period of α.*

In terms of homogeneous spaces, this means that the homogeneous space

V corresponding to α has a rational point in K if and only if $e(K/k)$ is divisible by its period.

COROLLARY 2. *Let A, A' be as in Corollary* 1. *Let V be a principal homogeneous space of A defined over k, of period prime to p. Then the index of V is equal to its period.*

Proof. There exist ramified extensions, e.g. $k(\pi^{1/e})$, with preassigned ramification index, whose degree is equal to that index.

To describe $\mathrm{Hom}(\Omega'_m, A'_m)$ more concretely is, of course, easy. We choose a generator ζ for Ω'_m. Then a homomorphism χ is determined by the image $\chi(\zeta)$ of ζ, and this may be any element of A'_m. In order that χ be a $G_{k'}$-homomorphism, it is necessary and sufficient that $\chi(\zeta^\sigma) = \sigma\chi(\zeta)$ for each $\sigma \in G_{k'}$. Defining the integer $\nu_\sigma \pmod m$ by $\zeta^\sigma = \zeta^{\nu\sigma}$, we see that the condition becomes $\nu_\sigma\chi(\zeta) = \sigma\chi(\zeta)$. Thus, $\mathrm{Hom}_{G_k}(\Omega'_m, A'_m)$ is isomorphic to the group of solutions $x \in A'_m$ of the equations $\sigma x = \nu_\sigma x$, $\sigma \in G_{k'}$. The isomorphism is not canonical, but depends on the choice of a primitive m-th root of unity ζ.

In particular, suppose that k' is a finite field with q elements. Then $G_{k'}$ has a canonical generator, namely the Frobenius automorphism $\xi \to \xi^q$. Its effect on an element x of A' is denoted by $x^{(q)}$. We may therefore express our result in this case as follows.

THEOREM 2. *Let A be an abelian variety defined over k with a non-degenerate reduction A', and suppose k' is a finite field with q elements. Then the group of elements of order prime to p in $H^1(k, A)$ is isomorphic to the group of solutions of $x^{(q)} = qx$ on A', of order prime to p.*

We observe that $x \to x^{(q)} - qx$ is an endomorphism of A'. Furthermore, if π denotes the Frobenius endomorphism of A', then its transpose ${}^t\pi$ on the Picard variety is easily seen to be given by the formula

$$ {}^t\pi y = q y^{(1/q)}. $$

Consequently, the transpose of $\pi - \delta$ is given by the endomorphism $y \to qy^{(1/q)} - y$ on $\hat{A}'$. Raising the kernel of this endomorphism to the q-th power, we see that the kernel is isomorphic to the subgroup of $\hat{A}'$ satisfying $y^{(q)} = qy$. In particular, we see that the group of solutions of $x^{(q)} = qx$ on A', of order prime to p, is dual to the group of rational points of $\hat{A}'$ in k', of order prime to p.

We close this section with an example of a homogeneous space whose index is not equal to its period. Suppose first of all that we could construct an abelian variety A over a field k such that $A_m \subset A_k$ and such that A_K is

divisible by m for each algebraic extension K of k. Then the Kummer sequence gives isomorphisms

$$\mathrm{Hom}(G_k, A_m) \approx H^1(k, A)_m$$

and, moreover, for each K/k, a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(G_k, A_m) & \approx & H^1(k, A)_m \\ \Big\downarrow \mathrm{res} & & \Big\downarrow \mathrm{res} \\ \mathrm{Hom}(G_K, A_m) & \approx & H^1(K, A)_m, \end{array}$$

where the left hand res means restriction of homomorphisms from G_k to G_K. If $f: G_K \to A_m$ is a homomorphism, we see that K splits the corresponding cohomology class if and only if G_K is in the kernel of f. Thus the index of the corresponding homogeneous space would be the *order* of the group $f(G_k)$, whereas its period would be the *exponent* of the group $f(G_k)$. In particular, if k has an abelian extension whose group is isomorphic to A_m, i.e. to the direct product of $2r$ cyclic groups of order m ($r = \dim A$), then we can construct a homogeneous space with index m^{2r} and period m.

An actual example can be constructed easily enough. Let A be defined over an algebraically closed field k_0. Define $k_i = k_{i-1}((t_i))$ (power series in one variable) for $1 \leqq i \leqq 2r$. One proves by induction that $A_{k_i} = mA_{k_i}$, and a similar divisibility statement for finite extensions. Then we can construct our example with $k = k_{2r}$ and the abelian extension $k(t_1^{1/m}, \cdots, t_{2r}^{1/m})$.

One could also construct a similar example over a purely transcendental function field in $2r$ variables. Incidentally, we note that the Kummer sequence shows, for any A and k, that if $A_m \subset A_k$ and $\mathrm{per}_k V = m$, then $\mathrm{ind}_k V$ divides m^{2r}. Thus our example is as bad as possible under the conditions $A_m \subset A_k$.

5. Global fields. Let k be a field with a fixed set of (inequivalent) discrete valuations $\mathfrak{p}$ which we shall call primes. By a prime in a finite algebraic extension K of k, we mean, of course, a valuation of K which extends a prime of k. Let m be a natural number not divisible by the characteristic of k. We shall say that k is an *m-global field* if each finite extension K of k has the following two properties.

(Gl1) If A is an abelian variety defined over K, then A has a non-degenerate reduction at all but a finite set of primes $\mathfrak{p}$ of K.

(Gl2, m) The set of primes of K dividing m is finite, and if S is any finite set of primes of K, there is only a finite number of abelian extensions of K of exponent m which are unramified outside S.

By well known elementary properties of number fields, one sees immediately that an algebraic number field of finite degree is m-global for every m, if we take as primes all the inequivalent discrete valuations.

The same remark applies to a field of algebraic functions of one variable over a finite constant field, and shows that it is m-global for m prime to its characteristic.

More generally, let k be an algebraic function field in n variables (the case $n = 0$ is not excluded) over a constant field k_0 such that $k_0^*/(k_0^*)^m$ is finite, for instance, a $\mathfrak{p}$-adic field, or an algebraically closed field. Choose as set of primes of k those arising from the prime divisors rational over k_0 of a projective normal model of k. Then it is easy to see (using results of algebraic geometry) that k is m-global.

Finally, if k is a function field over an algebraic number field of finite degree, then k is m-global for every m. The set of primes is then to be the set of prime divisors on a "mixed characteristic" model. This can easily be seen by reducing the proof to a geometric statement. As this, and the above fields are meant mostly to give concrete examples of m-global fields to the reader, we do not go in detail into the proofs that they are m-global, since they are essentially well known.

For the convenience of the reader, we indicate very briefly a sketch of the manner in which the above fields can be proved to satisfy our two global axioms.

(Gl 1) actually depends on the fact that an element of the field k has only a finite number of zeros and poles. To check that a reduction is non-degenerate, one checks that each property entering into the definition of an abelian variety has a non-degenerate reduction. For instance, we have: the absolute irreducibility (say of the Chow form if the variety is in projective space); the non-singularity (which depends on the non-vanishing of a determinant which is an element of k); the fact that some mappings are everywhere defined; associativity; etc.

As for (Gl 2), say for number fields, one may look at it either from the point of view that there is only a finite number of unramified extensions of degree m (abelian or non-abelian), a fact already stated in Hilbert's *Zahlbericht*, or from the point of view of Kummer theory: After adjoining the m-th roots of unity, the extension can be obtained by extracting radicals, and one uses the finiteness of class number and unit theorem. In the geometric case, one uses the analogous facts, which involve the Jacobian for the case of curves, and the Picard variety as well as the torsion part of the Neron-Severi group in higher dimension.

We shall now reprove for global fields the weak part of the Mordell-Weil theorem, i.e. Theorem 3 below.

PROPOSITION 10. *Let A be an abelian variety defined over a field k. Let m be prime to the characteristic of k and let $K = k(1/m \cdot A_k)$. Then $(A_k : mA_k)$ is finite if and only if $[K : k]$ is finite.*

Proof. It is trivial that if $(A_k : mA_k)$ is finite, then $[K : k]$ is finite. Conversely, consider the exact sequence

$$0 \to A_m \to A_K \to mA_K \to 0$$

Let $G = G(K/k)$. We have the cohomology sequence

$$0 \to A_m \cap A_k \to A_k \to mA_K \cap A_k \to H^1(G, A_m).$$

By assumption, $mA_K \cap A_k = A_k$, and thus we get the injection

$$0 \to A_k/mA_k \to H^1(G, A_m)$$

which shows that A_k/mA_k is finite.

COROLLARY. *Let A be an abelian variety defined over a field k, and let m be a natural number prime to the characteristic of k. Let L be a finite extension of k. If A_L/mA_L is finite then so is also A_k/mA_k.*

Proof. By the proposition, $L(1/m \cdot A_L)$ is finite over L. This implies a fortiori that $k(1/m \cdot A_k)$ is finite over k. Using the proposition once more, we get what we want.

THEOREM 3. *Let A be an abelian variety defined over an m-global field k. Then A_k/mA_k is finite.*

Proof. By the corollary, we may assume that $A_m \subset A_k$. Let $K = k(1/m \cdot A_k)$. By Proposition 9, we know that K/k is unramified at every prime $\mathfrak{p}$ not dividing m at which A has a non-degenerate reduction. From the definition of m-global, it follows that K is finite over k because it is abelian of exponent m over k. We now apply Proposition 10, to conclude the proof.

If K is a finite Galois extension of k, and if A is an abelian variety defined over k such that its group of rational points A_K in K is finitely generated (i.e. satisfies the strong Mordell-Weil theorem), then obviously $H^r(K/k, A)$ is finite for $r > 0$. However, Theorem 3 will suffice to prove the analogous result for m-global fields. For use in the statement of our next theorem, we recall that the m-primary part of an abelian group consists of those elements whose period divides a power of m.

THEOREM 4. *Let A be an abelian variety defined over an m-global*

field k. If K/k is a finite Galois extension, then the m-primary part of the group $H^r(K/k, A)$ is finite for each $r > 0$.

Proof. This is an immediate consequence of the following general cohomological fact.

LEMMA. *Let G be a finite group and X a G-module such that X/mX and X_m are finite. Then the m-primary part of $H^r(G, X)$ is finite for each $r > 0$.*

Proof. Since $H^r(G, X)$ is a torsion group of bounded exponent $(G: 1)$, it is enough to prove $H^r(G, X)_m$ finite. The map $m: X \to X$ can be written as a product $m = g \circ h$ of the maps g and h in the exact sequences

$$0 \to X_m \to X \xrightarrow{h} mX \to 0$$

$$0 \to mX \xrightarrow{g} X \to X/mX \to 0.$$

For the induced cohomology maps in dimension r, we have $m_* = g_* h_*$. From the exact cohomology sequences derived from our two exact sequences, we see that the kernels of h_* and g_* are finite, being homomorphic images of $H^r(G, X_m)$ and $H^{r-1}(G, X/mX)$ respectively. Consequently, the kernel of m_* is finite, which is what we wanted to prove.

If A is an abelian variety defined over an m-global field k, we say that an element $\alpha \in H^1(k, A)$ *splits at a prime* $\mathfrak{p}$ of k if α is in the kernel of the canonical map $H^1(k, A) \to H^1(k_\mathfrak{p}, A)$, where $k_\mathfrak{p}$ denotes the completion of k at $\mathfrak{p}$. In other words, α splits at $\mathfrak{p}$ if the corresponding homogeneous space has a rational point in $k_\mathfrak{p}$.

Selmer [11] has given examples of principal homogeneous spaces for abelian varieties of dimension 1 over the rational number field $\boldsymbol{Q}$ which split at all primes p but do not split in $\boldsymbol{Q}$. The elliptic curve $3X^3 + 4Y^3 + 5Z^3 = 0$ is such a space over its Jacobian. On the other hand, we can show that the number of such spaces with given period is finite. More precisely, let us denote by $H^1(k, A, S)$ the subgroup of $H^1(k, A)$ consisting of the elements which split at all primes outside a finite set S. We have

THEOREM 5. *Let A be an abelian variety defined over an m-global field k. Then $H^1(k, A, S)_m$ is finite.*

Proof. Without loss of generality, we may assume $A_m \subset A_k$. Indeed, the restriction of $H^1(k, A)$ to $H^1(K, A)$, where $K = k(A_m)$, has finite kernel by Theorem 4, and a fortiori that of $H^1(k, A, S)_m$ to $H^1(K, A, S)_m$. Furthermore, we may enlarge S until it contains all primes $\mathfrak{p}$ dividing m

and all primes $\mathfrak{p}$ where A does not have a non-degenerate reduction. Now for $\mathfrak{p} \notin S$, consider the commutative diagram

$$\begin{array}{ccccccc} 0 \to A_k/mA_k & \to & \mathrm{Hom}(G_k, A_m) & \to & H^1(k, A)_m & \to & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 \to A_{\mathfrak{p}}/mA_{\mathfrak{p}} & \to & \mathrm{Hom}(G_{\mathfrak{p}}, A_m) & \to & H^1(k_{\mathfrak{p}}, A)_m & \to & 0. \end{array}$$

Here we have abbreviated by $A_{\mathfrak{p}}$ the group $A_{k_{\mathfrak{p}}}$ and by $G_{\mathfrak{p}}$ the decomposition group $G_{k_{\mathfrak{p}}}$ which we may view as a subgroup of G_k, uniquely determined up to a conjugation. The horizontal arrows are the exact Kummer sequences and the vertical arrows are the canonical maps, the middle one therefore denoting simply the operation of restricting to $G_{\mathfrak{p}}$ a homomorphism of G_k. What we shall actually prove is that the inverse image of $H^1(k, A, S)_m$ in $\mathrm{Hom}(G_k, A_m)$ is finite. To this effect, it will be enough to show that if $\chi: G_k \to A_m$ is a homomorphism whose cohomology class in $H^1(k, A)$ splits outside S, then the abelian extension K_χ/k of exponent m which is cut out by the kernel of χ is unramified outside S. By the commutativity of the right square of the above diagram we know that the restriction of χ to $G_{\mathfrak{p}}$ is of the form $\chi(\sigma) = (\sigma - 1)(1/m \cdot a)$ for some $a \in A_{\mathfrak{p}}$. Thus we have $K_\chi \subset k_{\mathfrak{p}}(1/m \cdot a)$, and, by Proposition 9, it follows that K_χ is unramified at $\mathfrak{p}$. This completes the proof of Theorem 5.

It is natural to raise the question whether, given an element of $H^1(k_{\mathfrak{p}}, A)$, there exists an element of $H^1(k, A)$ which restricts to it. We can prove this in a special case.

THEOREM 6. *Let k be any field with a discrete valuation $\mathfrak{p}$ and let $k_{\mathfrak{p}}$ be its completion. Let m be prime to the characteristic of k and assume that the group of m-th roots of unity Ω_m lies in k. Let A be an abelian variety defined over k such that $A_m \subset A_k$. Then given $\alpha_{\mathfrak{p}} \in H^1(k_{\mathfrak{p}}, A)_m$, there exists an element $\alpha \in H^1(k, A)_m$ whose canonical image in $H^1(k_{\mathfrak{p}}, A)$ is $\alpha_{\mathfrak{p}}$.*

Proof. We use the Kummer sequence again, and the exact commutative diagram

$$\begin{array}{ccccc} \mathrm{Hom}(G_k, A_m) & \to & H^1(k, A)_m & \to & 0 \\ \downarrow & & \downarrow & & \\ \mathrm{Hom}(G_{\mathfrak{p}}, A_m) & \to & H^1(k_{\mathfrak{p}}, A)_m & \to & 0. \end{array}$$

We are trying to prove that the right hand vertical arrow is surjective. To do so, it is enough to prove the left hand vertical arrow is surjective. Since

A_m is isomorphic as an abstract group to the direct sum of $2r$ copies of Ω_m ($r = \dim A$), we have

$$\mathrm{Hom}(G, A_m) \approx (\mathrm{Hom}(G, \Omega_m))^{2r},$$

and, consequently, it is enough if we show the surjectivity of

$$\mathrm{Hom}(G_k, \Omega_m) \to \mathrm{Hom}(G_\mathfrak{p}, \Omega_m).$$

Recall now that Hom means here continuous homomorphisms, so that by the usual Kummer duality, we have $\mathrm{Hom}(G_k, \Omega_m) \approx k^*/(k^*)^m$, and similarly for $k_\mathfrak{p}$. Thus, we must simply show the surjectivity of $k^*/(k^*)^m \to k_\mathfrak{p}^*/(k_\mathfrak{p}^*)^m$. This is now obvious since $(k_\mathfrak{p}^*)^m$ is an open subgroup of $k_\mathfrak{p}^*$, m being prime to the characteristic.

Remark. Under the same hypotheses as in the theorem, one can deal with a finite number of discrete valuations, and use the approximation theorem to show that there is an α restricting simultaneously to a finite number of given $\alpha_{\mathfrak{p}_i}$.

In analogy with Grunwald's theorem in class field theory, one may conjecture that if k is an algebraic number field and $\mathfrak{p}$ a given prime, then given $\alpha_\mathfrak{p} \in H^1(k_\mathfrak{p}, A)$, there exists $\alpha \in H^1(k, A)$ restricting to $\alpha_\mathfrak{p}$.

Finally, we prove a result indicating that $H^1(k, A)$ is usually a large group when k is a global field.

THEOREM 7. *Let m be a natural number and let k be a field with an infinite number of abelian extensions of exponent exactly m. Let A be an abelian variety defined over k such that* (1) *A_k/mA_k is finite and* (2) *A_k contains at least one element a of exact period m. Then $H^1(k, A)$ contains an infinite number of elements of period m, and, in fact, an infinite number such that the corresponding homogeneous spaces have index m as well as period m.*

Proof. Let $L = k(1/m \cdot A_k)$. Since we have assumed A_k/mA_k finite, L is a finite extension of k. Consequently, by our hypothesis about the existence of abelian extensions of exponent m, there exists a Galois extension K of k linearly disjoint from L whose group $G = G(K/k)$ is the direct product of an arbitrarily large number of cyclic groups of order m. For each homomorphism χ of G into the cyclic group $\langle a \rangle$ of order m generated by a, let $\alpha_\chi \in H^1(K/k, A) \subset H^1(k, A)$ denote the cohomology class of the 1-cocycle $\sigma \to \chi(\sigma)$. We claim that the map $\chi \to \alpha_\chi$ is an injection. Indeed, if $\chi(\sigma) = (\sigma - 1)b$, $b \in A_k$, $\sigma \in G$, then $m\chi(\sigma) = (\sigma - 1)mb = 0$ for all σ; hence $mb \in A_k$. Since K is disjoint from L, it follows that $b \in A_k$ and $\chi = 0$.

Thus, $H^1(k, A)$ contains a subgroup isomorphic to $\mathrm{Hom}(G, \langle a \rangle)$, that is, to the direct product of arbitrarily many cyclic groups of order m. Moreover, for each element of this subgroup, the corresponding homogeneous space has index = period. This follows from the Corollary of Proposition 5, § 2 because, since $\langle a \rangle$ is cyclic, the index in G of the kernel of the homomorphism $\chi: G \to \langle a \rangle$ is equal to the period of χ, and the subfield of K cut out by this kernel splits α.

PARIS.

REFERENCES.

[1] A. Albert, "On primary normal division algebras of degree 8," *Bulletin of the American Mathematical Society*, vol. 39 (1933), pp. 265-272.

[2] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1956.

[3] F. Chatelet, "Méthode Galoisienne et courbes de genre 1," *Annales de l'Universite de Lyon*, Section A., t. 89 (1946), pp. 40-49.

[4] ———, "Variations sur un thème de Poincaré," *Annales de l'Ecole Normale superieure*, vol. 59 (1944), pp. 249-300.

[5] W. L. Chow and S. Lang, "On the birational equivalence of curves under specialization," *American Journal of Mathematics*, vol. 79, No. 3 (1957), pp. 649-652.

[6] J. Igusa, "Fibre systems of Jacobian varieties, II," *American Journal of Mathematics*, vol. 78 (1956), pp. 745-760.

[7] S. Lang, "Algebraic groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[8] E. Lutz, "Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques," *Journal für die reine und angewandte Mathematik*, Bd. 177 (1937), pp. 238-247.

[9] A. Mattuck, "Abelian varieties over p-adic ground fields," *Annals of Mathematics*, Series 2, vol. 62 (1955), pp. 92-119.

[10] P. Roquette, "Uber das Hassesche Klassenkorper-Zerlegungesetz," *Journal für die reine und angewandte Mathematik*, Bd. 197 (1957), pp. 49-67.

[11] E. Selmer, "The diophantine equation $ax^3 + by^3 + cz^3 = 0$," *Acta Mathematika*, vol. 85 (1951), pp. 203-362.

[12] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[13] A. Weil, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955), pp. 493-512.

[14] ———, "The field of definition of a variety," *American Journal of Mathematics*, vol. 78 (1956), pp. 509-524.

EXTENSIONS OF VECTOR GROUPS BY ABELIAN VARIETIES.*[1]

By MAXWELL ROSENLICHT.

This paper gives, among other things, the detailed proofs of a number of results previously announced by the author (cf. [10, § 5] and [11]; also [7, § 2] and [8]). The point of departure was the problem of finding a good geometric theory for the simple differentials of second kind on an algebraic variety. Such a theory, at least in the case of characteristic zero, is essentially contained (via the Albanese map) in the corresponding theory for abelian varieties, and it quickly became apparent that the proper object of study is the set of all algebraic group extensions of direct products of additive groups over a given abelian variety. The set of equivalence classes of extensions of the one-dimensional additive group by a given abelian variety A is naturally endowed with the structure of a vector space (over the universal domain), and the main results say that this vector space has the same dimension as A (Th. 3) and is naturally isomorphic to the cohomology space $H^1(A, \mathcal{O}_A)$, $\mathcal{O}_A$ being the sheaf of local rings on A (Th. 1). (A form of the first result that concerns the possible direct product decompositions of group extensions over A is misstated in our previous papers; this hinges on the fact that a product of additive groups may be susceptible of more than one vector space structure. The correct statement is in Prop. 11.) We leave aside the question of differentials of the second kind, concentrating on the matter of group extensions, but the relation between the two subjects can be gathered from the characteristic zero part of the proof of Prop. 11 (see Lemma 3 and the remark following the Prop.). This last mentioned part is the only place where our methods are not purely algebraic and where there is an essential difference between the case of characteristic zero and $p \neq 0$. A purely algebraic proof of the point in question could have been given, but would have been long. (Such a proof of the dimensionality of the space of extensions can be found in [1], a paper which is mostly restricted to characteristic zero and is in large part an algebraization of [8]; Barsotti has also published a proof of the same fact for characteristic $p \neq 0$ that is based on the infinitesimal

* Received January 21, 1958.

[1] This research was supported in large part by the U. S. Air Force through the Air Force Office of Scientific Research, part of the Air Research and Development Command under contract No. AF 18(600)-1571.

analysis of inseparable isogenies [2].) Some additional information on differentials of second kind can be found in an appendix where we prove some facts on the invariant differential forms on generalized jacobian varieties (stated without proof in [7] and [11]) which will have future utility.

A correspondence with J-P. Serre resulted in the simplification of some of the author's original ideas, as well as in a number of corrections. Serre will publish shortly some of his own contributions to the theory, notably the fact that the cohomology ring of an abelian variety (sheaf of local rings) is an exterior algebra. Part of a recent course of his ([16], to be published eventually in book form) was devoted to the present theory, and many sections here are very close to his notes (although there is a quite different proof of our Th. 1, whose full generality was discovered independently). We are especially indebted to Serre for certain of the useful trivialities on group extensions (beginning of our § 2) and for the exact sequences of Propositions 6 and 7.

1. Products of additive groups. The results of this section are probably well-known in the correct circles, although mainly unpublished. We have added something in the way of rationality statements and simplified proofs. The basic reference to linear algebraic groups is [3].

By a *vector group* we mean a commutative algebraic group G together with a regular operation of the multiplicative group G_m on G with the property that there exists a biregular birational correspondence between G and the ordinary affine space of the same dimension which is such that the group structure on G and the operation of G_m on G are those induced by the usual vector space structure on the affine space. It is clear what is meant by a *linear function on G, vector subgroup of G, linear homomorphism* (from one vector group into another), etc. If k is a field of definition for G as an algebraic group and for the operation of G_m on G, we say that k is a *field of definition for the vector group G*. Such being the case, any linear function on G is a linear combination with constant coefficients of linear functions that are defined over k, and if $n = \dim G$ it follows that functions $x_1, \cdots, x_n$ on G can be found such that the map $g \to (x_1(g), \cdots, x_n(g))$ is a biregular birational correspondence, defined over k, between G and the n-dimensional affine space and the vector group structure on G is given by the usual rules $x_i(g_1 + g_2) = x_i(g_1) + x_i(g_2)$, $x_i(cg) = cx_i(g)$; such functions $x_1, \cdots, x_n$ will be called *linear coordinate functions on G*.

The additive group G_a consists of the affine line with the composition law $(x_1)(x_2) = (x_1 + x_2)$. The additive parameter x on G_a is characterized to within multiplication by nonzero constants as an everywhere finite rational

function on G_a that vanishes to first order at the identity 0 and has no other zero. Thus G_a can be considered, in a well-defined way, to be a vector group. The algebraic group $(G_a)^n$ ($= G_a \times G_a \times \cdots \times G_a$, n times) can be endowed with the structure of a vector group (namely that induced by the natural vector group structure of each direct factor), but if $n > 1$ the group $(G_a)^n$ may possess various distinct vector group structures consistent with its underlying algebraic group structure. Functions $x_1, \cdots, x_n$ that are linear coordinate functions on $(G_a)^n$ with respect to one of its admissible vector group structures will be called *additive coordinate functions on* $(G_a)^n$.

Suppose we have a rational homomorphism $G_a \to G_a$. Fixing a coordinate function on G_a, this homomorphism is given by $x \to f(x)$, where $f(x)$ is a polynomial satisfying $f(x_1 + x_2) = f(x_1) + f(x_2)$. One deduces immediately that we can write

$$f(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_m x^{p^m},$$

where m is some positive integer, $a_0, \cdots, a_m$ are constants, and p is the field characteristic, if this differs from zero; in the case of characteristic zero, $f(x) = ax$, with a constant. In either case we call a function $f(x)$ of this form a *p-polynomial in* x (a term originally due to O. Ore), and we note that, conversely, any p-polynomial in x produces a rational endomorphism $G_a \to G_a$. As a consequence, if $\tau : (G_a)^n \to (G_a)^m$ is a rational homomorphism and $(x_1, \cdots, x_n)$, $(y_1, \cdots, y_m)$ are additive coordinate functions on the two groups, we have

$$y_i(\tau x) = f_{i1}(x_1) + \cdots + f_{in}(x_n), \qquad i = 1, \cdots, m,$$

where each f_{ij} is a p-polynomial in one variable. Such a function $f_{i1}(x_1) + \cdots + f_{in}(x_n)$ we call a *p-polynomial in* $x_1, \cdots, x_n$, and we note that, conversely, any m such p-polynomials in $x_1, \cdots, x_n$ give a rational homomorphism $\tau : (G_a)^n \to (G_a)^m$. In characteristic zero, a p-polynomial is a homogeneous linear function. All this implies that if $x_1, \cdots, x_n$ are additive coordinate functions on $(G_a)^n$ and $y_1, \cdots, y_n$ are rational functions on the same group, then this latter set is also a set of additive coordinate functions on $(G_a)^n$ if and only if each of the y's is a p-polynomial in the various x's, and conversely, each of the x's is a p-polynomial in the various y's. This enables us to find all possible admissible vector group structures on $(G_a)^n$, and it is clear that if the characteristic is $p \neq 0$ and $n > 1$, an infinite number of such vector group structures is possible, whereas in the case of characteristic zero the vector group structure is unique.

PROPOSITION 1. *Let H be a connected algebraic subgroup of $(G_a)^n$, k a field of definition for the solvability of H* (cf. [12, § 4]). *Then $(G_a)^n$ possesses an admissible vector group structure, also defined over k, with respect to which H is a vector subgroup.*

This is trivial if $\dim H = 0$, so suppose $\dim H > 0$. Then there exists an algebraic subgroup Γ of H which is biregularly isomorphic to G_a over k. Letting $x \in k(\Gamma)$ be an additive parameter on Γ and $x_1, \cdots, x_n$ be additive coordinates on $(G_a)^n$, each of the n functions $x_i(x)$ is a p-polynomial in x with coefficients in k, and not all $x_i(x)$ are zero. Consider coordinate changes on $(G_a)^n$ which interchange the coordinates $x_1, \cdots, x_n$, or which replace $x_1, \cdots, x_n$ by $x_1, x_2', \cdots, x_n'$, where each x_i' $(i = 2, \cdots, n)$ is the sum of x_i and a p-polynomial in $k[x_1]$. By interchanging $x_1, \cdots, x_n$, we can guarantee that the minimal degree of the nonzero $x_i(x)$'s is attained for $i = 1$, then by a coordinate change of the second type we can arrange that each nonzero $x_i(x)$, for $i > 1$, has degree less than that of $x_1(x)$. Hence, by repeated changes of this sort, we can insure that $x_i(x) = 0$ for $i = 2, \cdots, n$, which completes the proof if $\dim H = 1$. If $\dim H > 1$, we continue the same reasoning on $(G_a)^n/\Gamma$, etc.

The following proposition shows, among other things, that any algebraic group that is isogenous to a direct products of G_a's is also of this type, as is any homomorphic image of such a group. If such a group has k as a field of definition for its solvability, then it is biregularly isomorphic to a direct product of G_a's over k. Note that by [14, Prop. 5, Cor. 2], a perfect field of definition of such a group is always a field of definition for its solvability.

PROPOSITION 2. *Let the commutative algebraic group H be defined over k. If the characteristic is $p \neq 0$, suppose that $p \cdot h = 0$ for each $h \in H$, while if the characteristic is zero, suppose merely that H is linear and each of its elements is unipotent. Then there exists a biregular isomorphism, defined over k, from H into a direct product of G_a's.*

In the case of characteristic $p \neq 0$, the condition $p \cdot h = 0$ shows that no homomorphic image of H_0 is an abelian variety, so that here too H is linear and each of its elements is unipotent. Thus, in any case, we can suppose that H is a group of square matrices, each of which is of the form $I + \mu$, where I denotes the identity matrix, μ a nilpotent matrix (of order p if the characteristic is $p \neq 0$), and "$+$" ordinary addition of matrices, and where any two such matrices μ commute. Denoting by M the linear space spanned by all matrices μ such that $I + \mu \in H$, we get that M is defined over k and

is a commutative algebra under matrix multiplication each of whose elements is nilpotent (of order p if the characteristic is $p \neq 0$). The set G consisting of all matrices $I + m$, with $m \in M$, is a commutative algebraic group, defined over k and containing H. We prove that G is biregularly isomorphic over k to $(G_a)^n$, where $n = \dim M$. For this, note that $M \supset M^2 \supset M^3 \supset \cdots$, all these inclusions being proper until 0 is reached. Choose a basis $m_1, \cdots, m_n$ of M, each m_i being rational over k, such that for each $i = 1, \cdots, n-1$ the elements $m_{i+1}, \cdots, m_n$ span a subspace of M that is an M-submodule containing m_i^2. For any quantities $x_1, \cdots, x_n$, consider the expression $(\exp x_1 m_1) \cdots (\exp x_n m_n)$ (where in characteristic $p \neq 0$, exp denotes the first p terms of the exponential series); this clearly gives us a rational homomorphism defined over k from $(G_a)^n$ into G. It is easy to verify that

$$k((\exp x_1 m_1) \cdots (\exp x_n m_n)) = k(x_1, \cdots, x_n),$$

which completes the proof.

The remainder of this section is devoted to finding canonical forms for homomorphisms of products of G_a's.

LEMMA. *Let k be a field, $x_1, \cdots, x_n$ quantities that are algebraically independent over k, let $\nu_1, \cdots, \nu_n$ be integers > 0, and let $y_1, \cdots, y_n$ be elements of $k[x]$ such that $y_i - x_i^{\nu_i}$ is an element of $k[x]$ of total degree less than ν_i, $i = 1, \cdots, n$. Then $k(x)$ is an algebraic extension of $k(y)$ of degree $\nu_1 \nu_2 \cdots \nu_n$.*

We shall in fact prove more, namely that $k[x]$ is a free module over $k[y]$ having as generators the various quantities $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where $0 \leqq \alpha_i < \nu_i$, $i = 1, \cdots, n$. Let M be the $k[y]$-module generated by these quantities. Any power product of $x_1, \cdots, x_n$ can be written in the form $x_1^{\beta_1 \nu_1 + \alpha_1} \cdots x_n^{\beta_n \nu_n + \alpha_n}$, with $\beta_1, \cdots, \beta_n$ integers $\geqq 0$ and $\alpha_1, \cdots, \alpha_n$ as above, and this monomial differs from $y_1^{\beta_1} \cdots y_n^{\beta_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by an element of $k[x]$ of total degree $< \sum_{i=1}^n (\beta_i \nu_i + \alpha_i)$; thus each element of $k[x]$ can be written as an element of M plus another element of $k[x]$ of smaller total degree, and we deduce that $k[x] = M$. Finally, we must show that an expression

$$\sum_{\substack{\beta_1, \cdots, \beta_n \geqq 0 \\ 0 \leqq \alpha_i < \nu_i}} c_{\beta_1, \cdots, \beta_n, \alpha_1, \cdots, \alpha_n} y_1^{\beta_1} \cdots y_n^{\beta_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

(where each $c_{\beta,\alpha} \in k$ and not all are zero) cannot vanish. If Γ is the subset of $\{(\beta, \alpha)\}$ consisting of those $2n$-tuples (β, α) for which $c_{\beta,\alpha} \neq 0$ and

$\sum_{i=1}^{n}(\beta_i\nu_i+\alpha_i)$ is maximal, then the above expression is congruent modulo terms of lower total degree to

$$\sum_{(\beta,\alpha)\in\Gamma} c_{\beta,\alpha}x_1^{\beta_1\nu_1+\alpha_1}\cdots x_n^{\beta_n\nu_n+\alpha_n}.$$

But the various terms in this last sum are distinct, so our original sum is $\neq 0$.

PROPOSITION 3. *Let H be a vector group of dimension n, $\tau: H\to(G_a)^m$ a surjective rational homomorphism (of the additive structure of H only), all defined over the perfect field k of characteristic $p\neq 0$. Then there exist linear coordinate functions $x_1,\cdots,x_n$ on H and additive coordinate functions $y_1,\cdots,y_m$ on $(G_a)^m$, all defined over k, such that τ is given by*

$$y_i = x_i^{p^{\nu_i}} + (a\ p\text{-polynomial in } k[x] \text{ of degree} < p^{\nu_i}), \quad i=1,\cdots,m.$$

Furthermore, if τ is an isogeny, its degree is $p^{\nu_1}\cdots p^{\nu_n}$.

First pick any linear coordinate functions $x_1,\cdots,x_n$ on H and additive coordinate functions $y_1,\cdots,y_m$ on $(G_a)^m$, all defined over k, and write

$$y_i = u_i^{p^{\nu_i}} + (\text{a } p\text{-polynomial in } k[x] \text{ of degree} < p^{\nu_i}), \quad i=1,\cdots,m,$$

where $u_1,\cdots,u_m$ are each nonzero linear combinations of $x_1,\cdots,x_n$ with coefficients in k. Keep $x_1,\cdots,x_n$ fixed and alter the additive coordinate functions $y_1,\cdots,y_m$ on $(G_a)^m$ so that $(\nu_1,\nu_2,\cdots,\nu_m)$ is minimal in the lexicographical ordering, i.e., $y_1,\cdots,y_m$ are so chosen that ν_1 is minimal, ν_2 is minimal for this fixed ν_1, etc. Then $0\leqq\nu_1\leqq\cdots\leqq\nu_m$. If for some $i=2,\cdots,m$ we had u_i linearly dependent on $u_1,\cdots,u_{i-1}$, then by subtracting from y_i a suitable p-polynomial in $y_1,\cdots,y_{i-1}$, we could get new additive coordinate functions on $(G_a)^m$ giving rise to the same $\nu_1,\cdots,\nu_{i-1}$ and a strictly smaller ν_i; thus $u_1,\cdots,u_m$ are linearly independent. Hence we may alter our x's so that $x_1=u_1,\cdots,x_m=u_m$; all is now proved, except for the last statement, which comes from the lemma.

PROPOSITION 4. *Let $\tau:(G_a)^n\to(G_a)^m$ be a surjective rational homomorphism, defined over the infinite perfect field k of characteristic $p\neq 0$. Then there exist additive coordinate functions $x_1,\cdots,x_n$ on $(G_a)^n$ and $y_1,\cdots,y_m$ on $(G_a)^m$, all defined over k, such that τ is given by*

$$y_1 = x_1^{p^{\alpha_1}},\cdots,y_{m-1}=x_{m-1}^{p^{\alpha_{m-1}}},\quad y_m = x_m^{p^{\alpha_m}} + \sum_{s>0} c_s x_m^{p^{\alpha_m+s}},$$

where $0\leqq\alpha_1\leqq\cdots\leqq\alpha_m$ are integers and $c_1,c_2,\cdots\in k$.

Using Prop. 1, additive coordinate functions for $(G_a)^n$, all defined over k,

can be found such that the component of the identity of the kernel of τ is got by setting certain of these coordinate functions equal to zero. It follows that we can assume that τ is an isogeny, i.e., that its kernel is finite. (This implies, in particular, that $n = m$, but we shall maintain use of the two letters to distinguish the two groups involved.) The result is clear if $n \leqq 1$, so assume $n > 1$ and use induction. Take any additive coordinate functions on the two groups, say $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ respectively, all defined over k. Let α_1 be the greatest integer α such that $k[y] \subset (k[x])^{p^\alpha}$; since $k[x]$ is the ring of all everywhere finite rational functions on $(G_a)^n$ that are defined over k, and similarly for $k[y]$, the integer α_1 is independent of the choice of the x's and y's. When we express the y's as p-polynomials in the x's, all powers are at least to the p^{α_1}-th, and this power actually occurs. Choose elements $a_1, \cdots, a_n \in k$, not all zero, so that the one-parameter subgroup Γ of $(G_a)^n$ given by $x_1 = a_1 t, \cdots, x_n = a_n t$ meets the kernel of τ only at the identity and so that the degree of the map $\tau\colon \Gamma \to (G_a)^m$ is p^{α_1} (and no higher). By a linear change of the coordinates $x_1, \cdots, x_n$ we can assume that $a_1 = 1, a_2 = \cdots = a_n = 0$, and by a suitable change of $y_1, \cdots, y_m$, we can suppose that $\tau\Gamma$ is the subgroup $y_2 = \cdots = y_m = 0$ of $(G_a)^m$. Then $y_2, \cdots, y_m$ are independent of x_1 and y_1 is a linear combination of ${x_1}^{p^{\alpha_1}}$ and powers of $x_2, \cdots, x_n$ at least as high. Thus $y_1 = ({x_1}')^{p^{\alpha_1}}$, where ${x_1}'$ differs from a nonzero constant multiple of x_1 by a p-polynomial in $x_2, \cdots, x_n$. Altering x_1 to ${x_1}'$ we get $y_1 = {x_1}^{p^{\alpha_1}}$ and $y_2, \cdots, y_m \in k[x_2, \cdots, x_n]$, so that our induction assumption is applicable to the homomorphism $(G_a)^{n-1} \to (G_a)^{m-1}$ given by $(x_2, \cdots, x_n) \to (y_2, \cdots, y_m)$. We remark that a standard argument (considering $[k(y, x^{p^\nu}) : k(x^{p^\nu})]_i$, for various ν) shows the unicity of $\alpha_1, \cdots, \alpha_m$, and that we can dispense with the condition that k be infinite if the kernel of τ is connected.

2. Algebraic group extensions. Let G_1, G_2, G_3 be algebraic groups. A sequence of homomorphisms

$$G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3$$

will be called *exact* if, as usual, $\operatorname{Im} \phi_1 = \operatorname{Ker} \phi_2$ and, in addition, ϕ_1 and ϕ_2 are separable rational homomorphisms; similarly for longer sequences. If the above sequence is exact, then the corresponding sequence of Lie algebra homomorphisms

$$\mathfrak{g}_1 \to \mathfrak{g}_2 \to \mathfrak{g}_3$$

is also exact (e.g., cf. [13]). Conversely, if we are given a sequence of

rational homomorphisms of algebraic groups that is exact in the purely group-theoretic sense (i.e. we drop the condition that the various homomorphisms be separable) then we get a corresponding sequence of Lie algebra homomorphisms, and if the latter sequence is exact, so is the sequence of algebraic groups. (This amounts to showing that if $\psi: G \to G'$ is a purely inseparable isogeny of algebraic groups such that the corresponding Lie algebra map is an isomorphism, then ψ itself is a biregular isomorphism. This follows from the fact that we have an induced isomorphism between the spaces of local differentials at the identities of G and G' respectively, so ψ is separable.)

Let H and A be algebraic groups. By an *extension of H by A* (or *over A*) is meant an algebraic group G together with an exact sequence

$$0 \to H \to G \to A \to 0,$$

0 being the group with one element. Here H can be identified with a normal algebraic subgroup of G and A with G/H; when no confusion is possible, we shall often call G itself an extension of H by A. If the various groups and homomorphisms are defined over a field k, we say that the extension is *defined over k*. Another extension G' of H by A is called *equivalent* to the above extension if there exists a commutative diagram

$$\begin{array}{ccccccc} 0 \to & H & \longrightarrow & G & \longrightarrow & A & \to 0 \\ & \| & & \downarrow{\scriptstyle\psi} & & \| & \\ 0 \to & H & \longrightarrow & G' & \longrightarrow & A & \to 0, \end{array}$$

where ψ is a rational homomorphism and each of the two outside vertical maps is the identity; in this case, ψ is automatically a biregular isomorphism (for it is bijective, hence a purely inseparable isogeny, and the Lie algebra diagram associated with the above is commutative, so that ψ induces a Lie algebra isomorphism, hence is separable). The extension G of H by A is called *inessential* if, τ being the natural homomorphism from G to A, there exists a rational homomorphism $\phi: A \to G$ such that $\tau\phi = \text{identity}$. In this case, ϕ must be birational, so that A may be identified with an algebraic subgroup of G. This being done, we conclude from $G = HA$, $H \cap A = 0$, the separability of the homomorphism $A \to G/H$ and [12, Prop. 2] that the map $H \times A \to G$ defined by $h \times a \to ha$ is biregular.

If H and A are commutative algebraic groups, we shall denote by $\mathrm{Ext}(A,H)$ the set of equivalence classes of commutative extensions of H by A. (Much of what follows will go through under more general circumstances, namely that H be commutative and the restrictions of the inner

automorphisms of the extension group to H be given by a specific operation of A as a group of rational automorphisms of H. In any case, we are mainly interested in what happens when H is connected and commutative and A is an abelian variety, and here an extension group is always commutative [12, Th. 13, Cor. 2]; thus all algebraic groups in the remainder of § 2 will be assumed commutative.) We proceed to outline the functorial properties of $\mathrm{Ext}(A,H)$, leaving most of the details of proof to the reader. These details are all easy, except for the occasional question of separability, which is always to be handled by [12, Prop. 1]; at any rate, the next proposition is almost trivial from the point of view of factor systems (see below), which will be applicable in all special cases we later consider.

If $\phi: A' \to A$ is a rational homomorphism and $G \in \mathrm{Ext}(A,H)$, let G' be the subgroup of $A' \times G$ consisting of all $a' \times g$ such that a' and g have the same image in A. If we map H into G' by $h \to 0 \times h$, we get that G' is an extension of H by A'. Hence we have a map $\phi^*: \mathrm{Ext}(A,H) \to \mathrm{Ext}(A',H)$. If $\phi =$ identity, then $\phi^* =$ identity, and if $\phi': A'' \to A'$, then $(\phi\phi')^* = \phi'^*\phi^*$.

If $\psi: H \to H'$ is a rational homomorphism and $G \in \mathrm{Ext}(A,H)$, let $G' = G \times H'/\Delta$, where Δ is the kernel of the homomorphism $H \times H' \to H'$ defined by $h \times h' \to \psi h + h'$. If we map H' into G' by first mapping $h' \in H'$ into $0 \times h' \in G \times H'$, G' becomes an extension of H' by A. Hence we have a map $\psi_*: \mathrm{Ext}(A,H) \to \mathrm{Ext}(A,H')$. If ψ is the identity, so is ψ_*, and if $\psi': H' \to H''$, then $(\psi'\psi)_* = \psi'_*\psi_*$. In addition, if ϕ is as in the preceding paragraph, the two maps $\phi^*\psi_*, \psi_*\phi^*: \mathrm{Ext}(A,H) \to \mathrm{Ext}(A',H')$ are equal.

The method of Baer can now be used to put a composition law on $\mathrm{Ext}(A,H)$: If $G, G' \in \mathrm{Ext}(A,H)$, clearly $G \times G' \in \mathrm{Ext}(A \times A, H \times H)$. Let $\delta: A \to A \times A$ be the diagonal map and $\gamma: H \times H \to H$ be the group composition and set $G + G' = \delta^*\gamma_*(G \times G')$. This gives a map

$$\mathrm{Ext}(A,H) \times \mathrm{Ext}(A,H) \to \mathrm{Ext}(A,H)$$

which is clearly commutative and admits the trivial extension $A \times H$ as an identity. Associativity is established by reference to the map

$$\mathrm{Ext}(A,H) \times \mathrm{Ext}(A,H) \times \mathrm{Ext}(A,H) \to \mathrm{Ext}(A \times A \times A, H \times H \times H),$$

the diagonal map $A \to A \times A \times A$, and the group composition $H \times H \times H \to H$, while the inverse of an element of $\mathrm{Ext}(A,H)$ is obtained through the automorphism of H that sends h into $-h$. Thus $\mathrm{Ext}(A,H)$ is a commutative group. It is easy to verify that the maps ϕ^*, ψ_* of the two preceding paragraphs are homomorphisms, and equally straightforward, if slightly com-

plicated, to verify that if $\phi_1, \phi_2 : A' \to A$ then $(\phi_1 + \phi_2)^* = \phi_1^* + \phi_2^*$ and if $\psi_1, \psi_2 : H \to H'$ then $(\psi_1 + \psi_2)_* = \psi_{1*} + \psi_{2*}$. All this can be summarized as follows.

PROPOSITION 5. *If A, H are commutative algebraic groups, then the set* $\mathrm{Ext}(A, H)$, *together with the composition law given above, is a commutative group whose zero element is the trivial extension $A \times H$. With respect to this and the other operations given above,* $\mathrm{Ext}(A, H)$ *is a functor that is contravariant in A, covariant in H, and additive in both A and H.*

COROLLARY. $\mathrm{Ext}(A \times A', H) = \mathrm{Ext}(A, H) \times \mathrm{Ext}(A', H)$,

$$\mathrm{Ext}(A, H \times H') = \mathrm{Ext}(A, H) \times \mathrm{Ext}(A, H').$$

We denote by $\mathrm{Hom}(A, H)$ the group of rational homomorphisms from A into H. This clearly satisfies all the functorial properties in Prop. 5.

Now let $0 \to A' \to A \to A'' \to 0$ be an exact sequence of algebraic groups. For any $\tau \in \mathrm{Hom}(A', H)$, consider A to be an element of $\mathrm{Ext}(A'', A')$, and hence get $\tau_* A \in \mathrm{Ext}(A'', H)$. The map $\tau \to \tau_* A$ thus produces a canonical map

$$\mathrm{Hom}(A', H) \to \mathrm{Ext}(A'', H).$$

By Prop. 5, this map is a homomorphism, and is natural in the sense that a rational homomorphism $\psi : H \to H'$ produces the usual commutative diagram.

PROPOSITION 6. *Let $0 \to A' \to A \to A'' \to 0$ be an exact sequence of commutative algebraic groups and let H be another commutative algebraic group. Then the sequence of canonical homomorphisms*

$$0 \to \mathrm{Hom}(A'', H) \to \mathrm{Hom}(A, H) \to \mathrm{Hom}(A', H)$$
$$\to \mathrm{Ext}(A'', H) \to \mathrm{Ext}(A, H) \to \mathrm{Ext}(A', H)$$

is exact.

The proof of this is a long but largely mechanical recourse to the various definitions, hence will be omtited. Note that if we have a rational homomorphism $\psi : H \to H'$ and write the corresponding exact sequence for H', we get the usual commutative diagram. Each of the groups in the above exact sequence being a module with respect to the ring of rational endomorphisms of H, we see that the various homomorphisms are actually module homomorphisms. Later, we shall be concerned with the case $H = G_a$, and here the homomorphisms are vector space homomorphisms, the scalar field being the universal domain.

Analogously, consider an exact sequence of algebraic groups $0 \to H' \to H$

$\to H'' \to 0$. For any $\tau \in \mathrm{Hom}(A, H'')$, consider H to be an element of $\mathrm{Ext}(H'', H')$ and hence produce $\tau^* H \in \mathrm{Ext}(A, H')$. This map $\tau \to \tau^* H$ gives a canonical map

$$\mathrm{Hom}(A, H'') \to \mathrm{Ext}(A, H').$$

Again by Prop. 5, this map is a homomorphism, natural in the sense that a rational homomorphism $A' \to A$ produces the usual commutative diagram. Although it will not be used in this paper, the following analogue of Prop. 6 is included for completeness. The proof (omitted) is straightforward.

PROPOSITION 7. *Let* $0 \to H' \to H \to H'' \to 0$ *be an exact sequence of commutative algebraic groups and let* A *be another commutative algebraic group. Then the sequence of canonical homomorphisms*

$$0 \to \mathrm{Hom}(A, H') \to \mathrm{Hom}(A, H) \to \mathrm{Hom}(A, H'')$$
$$\to \mathrm{Ext}(A, H') \to \mathrm{Ext}(A, H) \to \mathrm{Ext}(A, H'')$$

is exact.

Before proceeding, we indicate one consequence of Prop. 6: In most of what follows, we shall be concerned mainly with $\mathrm{Ext}(A, H)$, where A is an abelian variety and H is a connected commutative algebraic group of unipotent matrices. Suppose, more generally, we consider $\mathrm{Ext}(G, H)$, where G is an extension of a torus by an abelian variety, and H is as above. Then we have an exact sequence $0 \to T \to G \to A \to 0$, with T a torus and A an abelian variety, so Prop. 6 gives the exact sequence

$$\mathrm{Hom}(T, H) \to \mathrm{Ext}(A, H) \to \mathrm{Ext}(G, H) \to \mathrm{Ext}(T, H).$$

Here the extreme groups are zero, so $\mathrm{Ext}(G, H)$ is isomorphic to $\mathrm{Ext}(A, H)$.

We now consider briefly the matter of factor systems. If $G \in \mathrm{Ext}(A, H)$ we call a rational map $\sigma: A \to G$ a *cross section* if $\tau\sigma =$ identity, τ being the canonical homomorphism $G \to A$. (By a rational map from one algebraic set, not necessarily irreducible, into another, we mean a law assigning to each component of the first set a rational map from that component into some component of the second algebraic set.) If $\sigma: A \to G$ is a cross section, then the map $A \times H \to G$ sending $a \times h$ into $\sigma a + h$ is birational (in the obvious sense) and we can define a rational map $f_\sigma: A \times A \to H$ by

$$f_\sigma(a_1, a_2) = \sigma a_1 + \sigma a_2 - \sigma(a_1 + a_2).$$

f_σ is a factor system, a *factor system* being a rational map $f: A \times A \to H$ satisfying the equation

$$f(a_1 + a_2, a_3) + f(a_1, a_2) = f(a_1, a_2 + a_3) + f(a_2, a_3),$$

and is symmetric ($f_\sigma(a_1, a_2) = f_\sigma(a_2, a_1)$). Conversely, if $f: A \times A \to H$ is a factor system, we can define a "normal law of composition" on $A \times H$ (obvious extension to reducible sets of the definition of [21]; associativity will correspond to the above equation) by

$$(a_1 \times h_1)(a_2 \times h_2) = (a_1 + a_2, h_1 + h_2 + f(a_1, a_2)),$$

and thus use [21] (with a slight additional argument if A and H are not both connected) to get an algebraic group G that is birationally equivalent to $A \times H$ and has the above composition as group law. If we map H into G by associating to any $h_1 \in H$ the point of G which has the effect on $A \times H$ of moving $a \times h$ into $a \times (h + h_1)$, it is clear that G becomes a central extension of H by A. Commutativity of G will correspond to symmetry of the factor system f, and the factor system f itself can be recovered from the cross section $\sigma: A \to G$ defined by $\sigma(a \times h) = a \times 0$ (a legitimate definition, since the map from $A \times H$ to G is biregular at almost all $a \times h$, and we can use the regular operation of H on both $A \times H$ and G to translate by $-h$). Thus *there is a one-one correspondence between cross sections of elements of* Ext (A, H) *and symmetric factor systems* $f: A \times A \to H$.

If $G \in \mathrm{Ext}(A, H)$ admits the cross section $\sigma: A \to G$, then for any rational map $u: A \to H$ we have a cross section σ' defined by $\sigma' a = \sigma a + ua$; conversely, any cross section $\sigma': A \to G$ is of this form. We get $f_{\sigma'}(a_1, a_2) = f_\sigma(a_1, a_2) + ua_1 + ua_2 - u(a_1 + a_2)$. The factor systems from $A \times A$ to H form a group and those of the form $(a_1, a_2) \to ua_1 + ua_2 - u(a_1 + a_2)$, for some rational map $u: A \to H$, form a subgroup, the group of *trivial factor systems*; the quotient group is the group of *classes of factor systems*. $G \in \mathrm{Ext}(A, H)$ corresponds to the trivial class if and only if there exists a cross section $\sigma: A \to G$ such that $f_\sigma = 0$; thus $\sigma(a_1 + a_2) = \sigma a_1 + \sigma a_2$ and we get $G = A \times H$.

Let $G \in \mathrm{Ext}(A, H)$ admit the cross section $\sigma: A \to G$ and let $\tau: G \to A$ be the canonical homomorphism. Then for any $g \in G$, the map $a \to \sigma(a + \tau g) - g$ is another cross section, which proves, in particular, that a cross section can be found that is defined at any given point of A. Let $\phi: A' \to A$ be a rational homomorphism such that σ is defined along each component of $\phi A'$. If $G' = \phi^* G$ is taken to be a subgroup of $A' \times G$ in the standard way, the map $\sigma': a' \to a' \times \sigma\phi a'$ is a cross section $\sigma': A' \to G'$ and the corresponding factor systems $f_\sigma: A \times A \to H$ and $f_{\sigma'}: A' \times A' \to H$ are related by $f_\sigma(a_1', a_2') = f_\sigma(\phi a_1', \phi a_2')$. Similarly, if we have a rational homomorphism $\psi: H \to H'$ and $G'' = \psi_* G$ is taken to be a quotient of $G \times H'$ in the standard way, the map $\sigma'': A \to G'$ obtained by first mapping a into $\sigma a \times 0$ is a cross section

and the factor system $f_{\sigma''}: A \times A \to H'$ is given by $f_{\sigma''}(a_1, a_2) = \psi f_\sigma(a_1, a_2)$. It follows that if $G_1, G_2 \in \mathrm{Ext}(A, H)$ correspond to factor systems f_1, f_2: $A \times A \to H$, then $G_1 + G_2$ corresponds to the factor system $f_1 + f_2$.

PROPOSITION 8. *If A, H are commutative algebraic groups, then the subset of* $\mathrm{Ext}(A, H)$ *consisting of those extensions which admit cross sections is a subgroup, naturally isomorphic to the group of classes of symmetric factor systems from $A \times A$ into H. If H is connected and linear, this subgroup is all of* $\mathrm{Ext}(A, H)$.

Only the last statement remains to be proved, and this follows from the cross section theorem [12, Th. 10]. Note that if A is an abelian variety and H is any connected commutative algebraic group, then *all* factor systems from $A \times A$ to H are symmetric: this comes from the fact that all extensions of H by A are commutative [12, Th. 13, Cor. 2].

3. Principal fiber spaces. For the convenience of the reader, as well as to fix terminology, we recall some concepts familiar in topology. Let H be an algebraic group that operates regularly on an algebraic set B, the operation being indicated by $(h, b) \to bh^{-1}$. B is called a *principal space with respect to* H [22] if the subset of $B \times B$ consisting of all points $b \times bh$ is closed and if there is an everywhere defined rational map θ from this subset into G such that $\theta(b \times bh) = h$. If, in addition, we have another algebraic set V and an everywhere defined surjective rational map $\pi: B \to V$, then B (more properly the triplet $\{B, V, \pi\}$) is called a *principal fiber space over V with group H* if, for any $b \in B$, $\pi^{-1}(\pi b)$ is precisely the orbit bH and if, for any $v \in V$, there exists a rational map $\sigma_v: V \to B$, defined in some neighborhood of v, such that $\pi\sigma_v = \text{identity}$. It is clear what is meant by *isomorphic* principal fiber spaces. If the local cross section $\sigma: V \to B$ is defined on the nonempty open subset U of V, the map $v \times h \to (\sigma v)h$ is clearly a biregular birational map between $U \times H$ and $\pi^{-1}U$. In particular, if V is irreducible, then it is the variety of H-orbits on B, in the sense of [12, Th. 2]. If $\{U_i\}_{i \in I}$ is a finite open covering of V and $\sigma_i: V \to B$ is a cross section that is everywhere defined on U_i then, for $v \in U_i \cap U_j$, we have $(\sigma_i v)h_i = (\sigma_j v)h_j$ if and only if $h_i = (s_{ij}v)h_j$, where $s_{ij}: V \to H$ is the rational map, regular on $U_i \cap U_j$, defined by $s_{ij}v = \theta(\sigma_i v, \sigma_j v)$, and $s_{ij}s_{jk} = s_{ik}$ for all $i, j, k \in I$. Conversely, such an open covering $\{U_i\}_{i \in I}$ of V and regular rational maps $s_{ij}: U_i \cap U_j \to H$ satisfying $s_{ij}s_{jk} = s_{ik}$ for all $i, j, k \in I$ give rise to a principal fiber space $B = \bigcup_{i \in I} U_i \times H$, with the points $v_i \times h_i \in U_i \times H$ and $v_j \times h_j \in U_j \times H$ identified if and only if $v_i = v_j$ and $h_i = (s_{ij}v_i)h_j$,

H operating on B by the rule $(h, v_i \times h_i) \to v_i \times h_i h^{-1}$ and $\pi(v_i \times h_i) = v_i$ (this is the definition of Weil [19]). As usual, two sets of transition functions $\{s_{ij}\}$ and $\{s'_{ij}\}$ with respect to the same open covering $\{U_i\}_{i \in I}$ of V give rise to isomorphic principal fiber spaces if and only if there exist everywhere regular rational maps $t_i: U_i \to H$ such that $s'_{ij} = t_i^{-1} s_{ij} t_j$, and the isomorphism class of the fiber space got from $\{U_i, s_{ij}\}$ is not altered by passing to a refinement of the covering $\{U_i\}$ and using the same $\{s_{ij}\}$. Thus (cf. [5, pp. 40 ff.]) the classes of principal fiber spaces over V with group H can be identified with the elements of the cohomology set $H^1(V, \mathfrak{H})$, where $\mathfrak{H}$ is the sheaf of germs of locally regular maps from V into H. If H is commutative, we have the usual commutative group structure on $H^1(V, \mathfrak{H})$ [15].

The simplest example of the preceding is the case of an algebraic group G and a connected solvable algebraic subgroup H, H operating on G by the rule $(h, g) \to gh^{-1}$. If π is the natural map from G to the left coset space G/H, then by [12, Th. 10] there exists a rational cross section $\sigma: G/H \to G$. If σ is regular on the nonempty open subset U of G/H and $g \in G$, then the map $v \to g^{-1}\sigma(gv)$ is a regular cross section on $g^{-1}U$. The various sets $g^{-1}U$ cover G/H, so G is indeed a principal fiber space.

Let A, H be commutative algebraic groups with H linear and connected. Any extension of H by A is a principal fiber space over A with group H, hence we have a well-defined map $\mathrm{Ext}(A, H) \to H^1(A, \mathfrak{H})$, $\mathfrak{H}$ being the sheaf of germs of locally regular maps from A into H. If A' is another commutative algebraic group and $\phi: A' \to A$ a rational homomorphism, we have induced homomorphisms $\phi^*: \mathrm{Ext}(A, H) \to \mathrm{Ext}(A', H)$, $\phi^{*\prime}: H^1(A, \mathfrak{H}) \to H^1(A', \mathfrak{H})$, and it is clear from the definition of ϕ^* that the diagram

$$\begin{array}{ccc} \mathrm{Ext}(A, H) & \to & H^1(A, \mathfrak{H}) \\ \downarrow & & \downarrow \\ \mathrm{Ext}(A', H) & \to & H^1(A', \mathfrak{H}) \end{array}$$

is commutative. (Cf. the cross section arguments immediately preceding Prop. 8.) Similarly, if H' is another connected commutative linear algebraic group and $\psi: H \to H'$ a rational homomorphism, we have induced homomorphisms $\psi_*: \mathrm{Ext}(A, H) \to \mathrm{Ext}(A, H')$, $\psi_*': H^1(A, \mathfrak{H}) \to H^1(A, \mathfrak{H}')$, and it follows directly from the definition of the former that the diagram

$$\begin{array}{ccc} \mathrm{Ext}(A, H) & \to & H^1(A, \mathfrak{H}) \\ \downarrow & & \downarrow \\ \mathrm{Ext}(A, H') & \to & H^1(A, \mathfrak{H}') \end{array}$$

is commutative. Referring to the definition of addition in $\mathrm{Ext}(A,H)$, we conclude that the map $\mathrm{Ext}(A,H)\to H^1(A,\mathfrak{H})$ is a homomorphism.

PROPOSITION 9. *Let A,H be commutative algebraic groups with H linear and connected and let $\mathfrak{H}$ be the sheaf of germs of locally regular maps from A into H. Then the canonical map*

$$\mathrm{Ext}(A,H)\to H^1(A,\mathfrak{H})$$

is a homomorphism. If A is an abelian variety, the map is injective.

All but the last statement is known. So suppose A abelian and that $G\in\mathrm{Ext}(A,H)$ gives rise to the zero cocycle. Then there is an everywhere regular cross section $\sigma\colon A\to G$, and we may assume that $\sigma\colon 0\to 0$. The complete subvariety σA of G generates an abelian variety, so σ must be a homomorphism. Hence G is trivial.

The homomorphism of Prop. 9 is natural in the sense that the commutative diagrams in the paragraph preceding it hold. In particular, if H is a vector group, the homomorphism is a vector space homomorphism. Note that if $H=G_a$, then $\mathfrak{H}$ is the sheaf of local rings $\mathfrak{O}_A$.

LEMMA. *Let A be an abelian variety, H a connected commutative linear algebraic group each of whose elements is unipotent, and $\mathfrak{H}$ the sheaf of germs of locally regular maps from A into H. Then each translation on A leaves fixed each element of $H^1(A,\mathfrak{H})$.*

The meaning of this is the following: Any $\xi\in H^1(A,\mathfrak{H})$ is determined by an open covering $\{U_i\}_{i\in I}$ of A and rational maps $\{s_{ij}\}_{i,j\in I}$ from A to H, each s_{ij} being regular on $U_i\cap U_j$, such that $s_{ij}+s_{jk}=s_{ik}$. For any $\alpha\in A$ and any rational function f on A, define the translated function $\lambda_\alpha f$ by $\lambda_\alpha f(a)=f(a-\alpha)$. The open covering $\{\alpha U_i\}$ of A and rational maps $\{\lambda_\alpha s_{ij}\}$ determine another element of $H^1(A,\mathfrak{H})$ which depends only on ξ and which we denote $\lambda_\alpha\xi$. We have to show that $\lambda_\alpha\xi=\xi$.

The lemma is trivial if $\dim H=0$. Let $\dim H=1$;* then $H=G_a$ and $H^1(A,\mathfrak{H})=H^1(A,\mathfrak{O}_A)$, a finite dimensional vector space over the universal domain (using, for example, [15, § 66, Th. 1] and the projective embeddibility of A [20]). For each $\alpha\in A$, λ_α is a linear transformation on $H^1(A,\mathfrak{O}_A)$; let Λ_α be the matrix of λ_α corresponding to a fixed basis $\xi_1,\cdots,\xi_r$ of $H^1(A,\mathfrak{O}_A)$. The map $\alpha\to\Lambda_\alpha$ is a homomorphism (not a priori rational) from A to $GL(r)$. Take an open covering $\{U_i\}$ of A, sufficiently fine so that $\xi_1,\cdots,\xi_r$ can be represented by sections $\{s_{ij}^{(1)}\},\cdots,\{s_{ij}^{(r)}\}$ regular on the respective $U_i\cap U_j$'s, and let k be a field of definition for A and each $s_{ij}^{(\nu)}$ such

that each U_i is k-open. Then each $\lambda_\alpha \xi_\nu$ is represented by a covering of A by $k(\alpha)$-open subsets and sections defined over $k(\alpha)$. By the unicity of the matrix Λ_α and the algebraic nature of the cohomology, Λ_α must be invariant under all $k(\alpha)$-automorphisms of the universal domain, hence must be purely inseparable over $k(\alpha)$. Take α generic for A over k and let q be a sufficiently high power of the field characteristic ($q = 1$ if the latter is 0). Then the matrix $\Lambda_\alpha^{(q)}$ (whose terms are the q-th powers of those of Λ_α) is rational over $k(\alpha)$ and $\alpha \to \Lambda_\alpha^{(q)}$ defines a rational map from A to $GL(r)$; by [12, Th. 3] this is a homomorphism, hence trivial. Thus $\lambda_\alpha \xi = \xi$ for all α, ξ, completing the proof for $\dim H = 1$. Note that the same argument shows that each translation on A leaves fixed each element of $H^m(A, \mathcal{O}_A)$ for any $m \geqq 0$.

Now take $\dim H > 1$ and use induction. Let H_1 be a connected one-dimensional algebraic subgroup of H. The sheaf $\mathcal{H}_1$ of germs of locally regular maps of A into H_1 is a subsheaf of $\mathcal{H}$ and, since H is a fiber space over H/H_1, the quotient sheaf $\mathcal{H}/\mathcal{H}_1$ can be identified with the sheaf of germs of locally regular maps of A into H/H_1. The exact sequence

$$0 \to \mathcal{H}_1 \to \mathcal{H} \to \mathcal{H}/\mathcal{H}_1 \to 0$$

gives rise [15, § 24, Prop. 6, Cor. 1] to the exact cohomology sequence

$$H^0(A, \mathcal{H}) \to H^0(A, \mathcal{H}/\mathcal{H}_1) \to H^1(A, \mathcal{H}_1) \to H^1(A, \mathcal{H}) \to H^1(A, \mathcal{H}/\mathcal{H}_1).$$

Note that translation by an $\alpha \in A$ induces an endomorphism λ_α of each of the above cohomology groups, these endomorphisms being allowed with respect to the above exact sequence, i.e. producing the usual commutative diagram. Now $H^0(A, \mathcal{H})$ consists of all everywhere regular maps from A to H. All such maps being constant, $H^0(A, \mathcal{H})$ is isomorphic to H, and similarly $H^0(A, \mathcal{H}/\mathcal{H}_1)$ is isomorphic to H/H_1. Thus $H^0(A, \mathcal{H}) \to H^0(A, \mathcal{H}/\mathcal{H}_1)$ is surjective and we have the exact sequence

$$0 \to H^1(A, \mathcal{H}_1) \to H^1(A, \mathcal{H}) \to H^1(A, \mathcal{H}/\mathcal{H}_1).$$

Let ξ be a fixed element of $H^1(A, \mathcal{H})$. Letting τ be the last homomorphism above, for any $\alpha \in A$, our induction assumption gives $\lambda_\alpha \tau \xi = \tau \xi$, so $\tau(\lambda_\alpha \xi - \xi) = 0$, i.e., $\lambda_\alpha \xi - \xi \in H^1(A, \mathcal{H}_1)$. For any $\beta \in A$, $\lambda_\beta(\lambda_\alpha \xi - \xi) = \lambda_\alpha \xi - \xi$, so the map $\alpha \to \lambda_\alpha \xi - \xi$ is a (purely group-theoretic) homomorphism from A to $H^1(A, \mathcal{H}_1)$. Since $\mathcal{H}_1$ is isomorphic to $\mathcal{O}_A$, $H^1(A, \mathcal{H}_1)$ is a vector space with a basis $\xi_1, \cdots, \xi_r$. Choose an open covering $\{U_i\}$ of A so fine that $\xi_1, \cdots, \xi_r, \xi$ can be represented by sections $\{s_{ij}^{(1)}\}, \cdots, \{s_{ij}^{(r)}\}$, $\{s_{ij}\}$ regular on the respective $U_i \cap U_j$'s (into $H_1, \cdots, H_1, H$ respectively), and let k be

a field of definition for everything here. Writing $\lambda_a\xi - \xi = c_1(a)\xi_1 + \cdots + c_r(a)\xi_r$, for suitable (unique) constants $c_1(a), \cdots, c_r(a)$, we see as before that $c_1(a), \cdots, c_r(a)$ are invariant under all $k(a)$-automorphisms of the universal domain, hence are purely inseparable over $k(a)$. Again taking a to be generic for A over k and q to be a sufficiently high power of the field characteristic (or 1 if the characteristic is 0), we have $(c_i(a))^q \in k(a)$ for $i = 1, \cdots, r$. Again by [12, Th. 3] $a \to (c_i(a))^q$ is a rational homomorphism from A into G_a, hence trivial. Thus each $c_i(a) = 0$, completing the proof that $\lambda_a\xi = \xi$.

THEOREM 1. *Let A be an abelian variety, H a connected commutative linear algebraic group each of whose elements is unipotent, and $\mathfrak{H}$ the sheaf of germs of locally regular maps from A into H. Then the canonical homomorphism*

$$\mathrm{Ext}(A, H) \to H^1(A, \mathfrak{H})$$

is bijective.

Injectiveness has been proved in Prop. 9, so it remains only to show that any principal fiber space over A with group H can be endowed with the structure of an element of $\mathrm{Ext}(A, H)$ in a manner consistent with the fibre space structure. Let V be such a principal fiber space, $\pi: V \to A$ the projection. Define a *translation* on V to be a biregular map $T: V \to V$ such that $(Tv)h = T(vh)$ for all $v \in V$, $h \in H$ and such that $\pi Tv - \pi v$ is constant (i.e. T is a bundle map lifting to V a translation on A). The translations on V form a group, the set of maps of the form $v \to vh_0$, for fixed $h_0 \in H$, a subgroup. The lemma says merely that any translation on A can be lifted to one on V; thus the group of translations on V is transitive. Now suppose that T is a translation on V possessing a fixed point. Then $\pi Tv = \pi v$ for all $v \in V$, so if θ is the map of the locus of $v \times vh$ on $V \times V$ such that $\theta(v \times vh) = h$, we have θ defined at $Tv \times v$. But $\theta(T(vh) \times vh) = \theta(Tv \times v)$, so there exist a rational map $\phi: A \to H$ such that $\theta(Tv \times v) = \phi\pi v$. Since V is locally a direct product and the map $v \to \theta(Tv \times v)$ is everywhere defined, so is the map ϕ; hence ϕ is a constant, which can only be zero, so $Tv = v$. Thus there exists one and only one translation on V carrying any one given point into another. Fix a point $e \in V$ such that $\pi e = 0$. For any $v \in V$, denote by T_v the translation on V satisfying $T_v e = v$. The one-one correspondence $v \to T_v$ puts a group structure on V having e as identity element, and we have to show that this group structure is algebraic. Let k be an algebraically closed field of definition for V, H, A, the operation of H on V, and π such that e is rational over k. Let w be a generic point of V over k

and $k(x)$ the smallest overfield of k which is a field of definition for T_w[2]; then $k(x)$ is a regular extension of k containing $k(w)$ and (since T_w is unaltered by any $k(w)$-automorphism of the universal domain) purely inseparable over $k(w)$. Hence we have a variety X and generically surjective rational maps $\tau: X \to V$, $\phi: X \times V \to V$, all defined over k and the former purely inseparable, such that if $x \times v$ is generic for $X \times V$ over k then $k(x)$ is the smallest overfield of k that is a field of definition for $T_{\tau x}$ and $\phi(x \times v) = T_{\tau x} v$. We have $k(x, T_{\tau x} v) = k(x, v)$, and if y is generic for X over $k(x, v)$, then $T_{\tau x}(T_{\tau y} v) = T_{\tau z} v$ for some generic point z of X over k, z depending only on x and y (conditions TG1 and TG2′ of [21]). By Prop. 2 of [21], X is a pregroup with respect to the composition law $x \times y \to z$ and V a pretransformation space for X with composition law $x \times v \to T_{\tau x} v$. Without loss of generality, we may suppose that X is already an algebraic group. Now for any $x \in X$, the map $v \to \phi(x \times v)$ is a translation on V, since this is so whenever x is generic for X over k, and similarly, any translation on V comes in this manner from an element of X. But there exists a nonempty open subset of V which is biregularly equivalent to an open subset of a birational model of V on which X operates regularly and the translates of this open subset of V cover V. Hence X operates regularly on V. For $x \times v$ generic for $X \times V$ over k, we have $\phi(x \times v) = T_{\tau x} v$; hence $\phi(x \times e) = T_{\tau x} e = \tau x$. Thus τ is everywhere defined and the equation $\phi(x \times v) = T_{\tau x} v$ holds for all $x \in X$, $v \in V$; τ is thus a homomorphism, one-one since it is purely inseparable. The rational homomorphism $\pi\tau: X \to A$ has as kernel all $x \in X$ for which $T_{\tau x}$ is a translation by an element of H; the kernel being commutative and A abelian, X is commutative. Let x, y be independent generic points of X over k. Then $\tau(xy) = T_{\tau x}(\tau y)$ is rational over $k(x, \tau y)$. Since $xy = yx$, we get $k(\tau(xy)) \subset k(x, \tau y) \cap k(\tau x, y) = k(\tau x, \tau y)$. (For the last step, let $\{\xi_i\}$, $\{\eta_j\}$ be bases for $k(x)/k(\tau x)$ and $k(y)/k(\tau y)$ respectively, with $\xi_1 = \eta_1 = 1$, and use the fact that $\{\xi_i \eta_j\}$ is a basis for $k(x, y)/k(\tau x, \tau y)$.) Thus $T_{\tau x}$ is defined over $k(\tau x)$, so $k(\tau x) = k(x)$ and τ is birational, hence also biregular. Map H into the group V by the rule $h \to eh$. The group law on V agrees with the operation of H on V and π is now a separable rational homomorphism with kernel H, completing the proof.

---

[2] The main point of the rest of the proof is to show that $k(x)$ is actually $k(w)$. A proof different from the one that follows can be constructed by sharpening the lemma to bring in fields of rationality: we would need a result stating that a bounding cocycle that is rational over a certain field is the boundary of a cochain rational over the same field. But this would involve a lengthy re-working of parts of [15] and would take us too far afield.

The main point in the above proof, to the effect that any principal fiber space over the abelian variety A with group H is a group extension of H by A, is well known to be false if H is the multiplicative group G_m, and counterexamples can also be given if H is connected and unipotent, but not commutative.

4. Extensions of G_a by an abelian variety. If A is an abelian variety, the group $\mathrm{Ext}(A, G_a)$ has the structure of a vector space (over the universal domain), isomorphic to $H^1(A, \mathcal{O}_A)$. The following proposition will settle at the beginning all rationality questions.

PROPOSITION 10. *Let A be an abelian variety that is defined over k. Then the elements of $\mathrm{Ext}(A, G_a)$ arising from extensions of G_a by A that are defined over k span $\mathrm{Ext}(A, G_a)$. Furthermore, any number of such elements are linearly dependent only if they are linearly dependent over k.*

Let $\mathfrak{U} = \{U_i\}_{i \in I}$ be a finite open covering of A by affine subsets that are defined over k. Then $H^1(A, \mathcal{O}_A)$ and $H^1(\mathfrak{U}, \mathcal{O}_A)$ are isomorphic [15, § 47, Th. 4], so any element of $H^1(A, \mathcal{O}_A)$ can be defined by a cocycle for the covering $\mathfrak{U}$, i.e. by a set $\{f_{ij}\}_{i,j \in I}$, where f_{ij} is an everywhere regular function on $U_i \cap U_j$ and $f_{ik} = f_{ij} + f_{jk}$ for all $i, j, k \in I$. Each f_{ij} has all its poles on a k-closed subset of A, hence [17, Th. 10, p. 239] is a linear combination with constant coefficients of elements of $k(A)$. Choose constants $\alpha_1, \cdots, \alpha_N$ that are linearly independent over k and functions $f_{ij}^{(\nu)} \in k(A)$ $(i, j \in I;\ \nu = 1, \cdots, N)$ such that $f_{ij} = \sum_{\nu=1}^{N} \alpha_\nu f_{ij}^{(\nu)}$ for all $i, j \in I$. Then $f_{ij}^{(\nu)}$ is everywhere regular on $U_i \cap U_j$ and for each $\nu = 1, \cdots, N$, $\{f_{ij}^{(\nu)}\}_{i,j \in I}$ is a cocycle for the covering $\mathfrak{U}$ of A. Thus $H^1(A, \mathcal{O}_A)$ is spanned by those of its elements that come from principal fiber spaces over A with group G_a that are defined over k. For any such fiber space V, we may choose a point $e \in V$ lying over $0 \in A$ that is rational over k and get an algebraic group structure on V having e as identity element and consistent with the fiber space structure; by the proof of Th. 1, this group structure is unique, hence invariant under all k-automorphisms of the universal domain, hence defined over a purely inseparable extension of k. (Actually, this group structure can be shown to be defined over k; cf. footnote 2). This proves the first statement of the proposition if k is algebraically closed. For any k, any extension of G_a by A that is defined over k possesses a cross section that is defined over k (G_a having k as a field of definition for its solvability), hence is describable by a factor system $f: A \times A \to G_a$ that is defined over k. We have proved that $\mathrm{Ext}(A, G_a)$ is spanned by elements associated with factor systems $f: A \times A$

$\to G_a$ that are defined over the algebraic closure of k. But for such an f, we can write $f = \sum \alpha_\nu f_\nu$, where $\{\alpha_\nu\}$ is a finite set of quantities that are linearly independent over k and where each f_ν is a function on $A \times A$ that is defined over k. Writing down the equation f satisfies as a factor system and using linear disjointness, we get that each f_ν is a factor system, which completes the proof of the first statement. It remains to show that if $f_1, \cdots, f_r$ are factor systems from $A \times A$ to G_a that are defined over k and if there exist constants $c_1, \cdots, c_r$, not all zero, such that $\sum_{i=1}^r c_i f_i$ is a trivial factor system, then such constants $c_1, \cdots, c_r$ may be found in k. For this, suppose $\sum_{i=1}^r c_i f_i(a_1, a_2) = u(a_1) + u(a_2) - u(a_1 + a_2)$, where u is a rational function on A. Each f_i being defined over k, hence having poles that are algebraic over k, we get that all the poles of u are algebraic over k. Hence there exist constants $d_1, \cdots, d_s$ and functions $u_1, \cdots, u_s$ on A that are defined over k such that $u = \sum_{i=1}^s d_i u_i$. Let $\alpha_1, \cdots, \alpha_N$ be a basis for the vector space over k spanned by $c_1, \cdots, c_r, d_1, \cdots, d_s$ and write $c_i = \sum_{j=1}^N c_{ij}\alpha_j$ for $i = 1, \cdots, r$ and $d_i = \sum_{j=1}^N d_{ij}\alpha_j$ for $i = 1, \cdots, s$, with each c_{ij} and d_{ij} in k. Linear disjointness gives

$$\sum_{i=1}^r c_{ij} f_i(a_1, a_2) = \sum_{i=1}^s d_{ij}(u_i(a_1) + u_i(a_2) - u_i(a_1 + a_2))$$

for each j, completing the proof.

LEMMA 1. *Let H, N be connected algebraic subgroups of the algebraic group G, with N normal in G, $G = HN$, and $H \cap N$ finite. Then the restriction to H of the natural homomorphism $G \to G/N$ is an isogeny whose degree is the Kronecker index $\mathrm{I}(H \cdot N)$.*

By [12, Prop. 2] we have an isogeny, the inseparable part q of whose degree is given by $H \cdot N = q(H \cap N)$. To get the lemma, note that the separable part of the degree of this isogeny is the number of points in $H \cap N$.

LEMMA 2. *Let the algebraic group G be an extension of $(G_a)^n$ by the abelian variety A and let the field characteristic be $p \neq 0$. Then $G = (G_a)^n B$, where B is the maximal abelian subvariety of G, and $(G_a)^n \cap B$ is finite. Furthermore, there exists an isogeny $A^{(p)} \to B$ ($A^{(p)}$ being the abelian variety got from A by taking p-th powers of coordinates) which composes with the natural isogeny $B \to A$ (restriction to B of $G \to A$) to give the map $a^{(p)} \to pa$.*

Let $\tau: G \to A$ be the natural homomorphism, $\sigma: A \to G$ a rational cross section, k a field of definition for everything, and a a generic point of A over k. The map $a \to p\sigma a$ is clearly independent of the choice of the cross section σ; since there exists such a σ that is regular over any given point of

A, we have an everywhere regular map $A \to B$, B being the image of G under the homomorphism $g \to pg$. B is clearly the maximal abelian subvariety of G, $(G_a)^n \cap B$ is finite (being both complete and linear), and $G = (G_a)^n B$ (by dimensions). But according to the theory of symmetric functions [18, Lemma 4, p. 13], the point $p\sigma a$ is rational over $k(a^{(p)})$, hence we have a homomorphism $\psi: A^{(p)} \to B$ and $\tau\psi a^{(p)} = \tau p\sigma a = pa$.

Note that the homomorphism $\phi: A^{(p)} \to A$ defined by $\phi a^{(p)} = pa$ induces a homomorphism $\phi^*: \mathrm{Ext}(A, G_a) \to \mathrm{Ext}(A^{(p)}, G_a)$, and Lemma 2 is practically equivalent to the statement that $\phi^* = 0$. Note also that nothing like the lemma is true in characteristic zero, for in that case, any finite subgroup of $(G_a)^n$ consists of 0 alone and the lemma can apply only to the trivial extension.

Let G be an extension of the *vector group* H by the abelian variety A. We call G *decomposable* if we can write $G = G_1 \times H'$, where G_1 is an extension of a vector subgroup H_1 of H by A and H' is a vector subgroup of H of dimension > 0; otherwise G is *indecomposable.*

LEMMA 3. *Let A be an abelian variety, H a vector group of dimension greater than A, and G an extension of H by A. Then G is decomposable.*

Let $\dim H = n$, $\dim A = \nu < n$, and first suppose that everything is defined over a perfect field k of characteristic $p \neq 0$. If a is generic for A over k, then $[k(a): k(pa)] = p^{2\nu}$ and $[k(a): k(a^{(p)})] = p^{\nu}$, so $[k(a^{(p)}): k(pa)] = p^{\nu}$. By Lemma 2, $G = HB$, B being the maximal abelian subvariety of G, and the isogeny $B \to A$ has degree dividing p^{ν}. Using the symmetry in Lemma 1, we obtain that the isogeny $H \to G/B$ also has degree dividing p^{ν}. Now use Prop. 3 to find linear coordinate functions $x_1, \cdots, x_n$ on H and additive coordinate functions $y_1, \cdots, y_n$ on G/B such that $H \to G/B$ is given by

$$y_i = x_i^{p^{\nu_i}} + (\text{a } p\text{-polynomial in } k[x] \text{ of degree} < p^{\nu_i}),\ i = 1, \cdots, n.$$

The degree of the isogeny $H \to G/B$ is $p^{\nu_1} \cdots p^{\nu_n} \leqq p^{\nu} < p^n$, so at least one of the ν_i's, say ν_1, is 0. Then $y_1 = x_1$. Let H' be the vector subgroup of H determined by $x_2 = \cdots = x_n = 0$, H_1 the vector subgroup determined by $x_1 = 0$, and $G_1 = H_1 B$. Then $G = G_1 H'$ and the homomorphism $H' \to G/G_1$ (which can be decomposed into $H' \to G/B \to (G/B)/(G_1/B)$) is given by $x_1 \to x_1$, i.e. is a biregular isomorphism, so $G = G_1 \times H'$.

It remains to consider the case of characteristic zero. For simplicity, and also to illustrate the connection of the present theory with that of differentials of the second kind, we assume, as we may, that the universal domain is the field of complex numbers and give an easy transcendental

proof. Let ω be an invariant differential (of degree one) on G and $\sigma: A \to G$ a rational cross section. The induced differential $\sigma^*\omega$ on A is closed, since ω is. If $\sigma': A \to G$ is another cross section then $\sigma' a = \sigma a + fa$, where $f: A \to H$ is a rational map, and conversely, any such f defines such a σ'. We know that $\sigma'^*\omega = \sigma^*\omega + f^*\omega$ (e.g. see the last paragraph of [13]; here $(f^*\omega)(a) = \omega(fa)$), that $f^*\omega$ is exact (coming as it does from an invariant differential on H), and for any $P \in A$, such a σ' exists that is finite at P; thus $\sigma^*\omega$ differs by an exact differential from a differential that is regular at P, i.e. $\sigma^*\omega$ is of the second kind. The dimension of the space of invariant differentials on G exceeds the first Betti number of A ($\dim G = n + \nu > 2 \dim A$), so there exists an invariant $\omega \neq 0$ on G such that $\sigma^*\omega$ has zero periods. $\sigma^*\omega$ is thus exact. Also, the differential induced on H by ω is not zero (for then ω would come from an invariant differential on A, which would have to be zero), so we can modify σ to obtain $\sigma^*\omega = 0$. Taking a suitable translate of σA, we get a subvariety W of G that passes through 0, maps into A in a generically surjective fashion, and has the differential zero induced on it by ω. These same facts are then true of the algebraic group G_1 generated by W (again use last paragraph of [13]). In particular, $G_1 \neq G$, and if we set $H_1 = G_1 \cap H$, H' a vector subgroup of H complementary to H_1, we get $G = G_1 \times H'$.

PROPOSITION 11. *Let A be an abelian variety. Then there exists a vector group H of dimension $\leqq \dim A$ and an indecomposable extension Γ of H by A such that any indecomposable extension of a vector group by A is isomorphic to the quotient of Γ by a vector subgroup of H. Furthermore, if we associate to each linear functional $\psi: H \to G_a$ the extension $\psi_*\Gamma \in \mathrm{Ext}(A, G_a)$, we obtain a vector space isomorphism between the dual space of H and* $\mathrm{Ext}(A, G_a)$.

Suppose $f_i: A \times A \to G_a$, $i = 1, \cdots, n$, are factor systems. Then we get a factor system $f: A \times A \to (G_a)^n$ by setting

$$f(a_1, a_2) = (f_1(a_1, a_2), \cdots, f_n(a_1, a_2)),$$

and this can be considered as a factor system from $A \times A$ to a vector group of dimension n with a fixed linear coordinate system. Hence $f_1, \cdots, f_n$ give rise to a well-defined extension G of an n-dimensional vector group by A, and clearly any such extension G can be so obtained. We do not alter G by adding to any f_i a trivial factor system, nor are the isomorphism class of G and the vector group structure of its maximal connected linear algebraic subgroup changed by juggling $f_1, \cdots, f_n$ by a nonsingular linear transformation

with constant coefficients. If $f_n = 0$, then G is the product of the extension of an $(n-1)$-dimensional vector group by A determined by $f_1, \cdots, f_{n-1}$ and the vector group G_a, i.e. G is decomposable, and conversely, if G is decomposable, then some nontrivial linear combination of $f_1, \cdots, f_n$ must be a trivial factor system; thus G is indecomposable if and only if the elements of $\mathrm{Ext}(A, G_a)$ determined by $f_1, \cdots, f_n$ (cf. Prop. 8) are linearly independent. The previous Lemma 3 now gives $\dim \mathrm{Ext}(A, G_a) \leqq \dim A$. If we construct an extension of a vector group by A by means of a set of factor systems corresponding to a basis of $\mathrm{Ext}(A, G_a)$, we get an indecomposable extension Γ of maximal dimension. It is now trivial to verify the various contentions of the proposition for this Γ.

Remark. It will be shown shortly (Th. 3) that equality holds above, i.e. $\dim H = \dim A$. Reference to the proof of the previous Lemma 3 shows that this equality, in the case of characteristic zero, implies that the dimension of the vector space of simple differentials of second kind on A modulo exact differentials is $2 \dim A$. In the case of characteristic $p \neq 0$, on the other hand, if we write $\Gamma = HB$, B being the maximal abelian subvariety of Γ we deduce that the isogeny $A^{(p)} \to B$ of Lemma 2 is actually a biregular isomorphism and that the covering $B \to A$ is exactly like $A^{(p)} \to A$, with $a^{(p)} \to pa$; furthermore, each of the ν_i in Lemma 3 must equal 1, so that there exist linear coordinate functions $x_1, \cdots, x_n$ $(n = \dim A)$ on H and additive coordinate functions $y_1, \cdots, y_n$ on Γ/B so that the isogeny $H \to \Gamma/B$ is given by

$$y_i = x_i^p + c_{i1}x_1 + \cdots + c_{in}x_n, \qquad i = 1, \cdots, n, \text{ all } c_{ij} \text{ constant.}$$

Finally, we note that in certain problems, we may not be interested in any specific vector group structure of a subgroup but merely in what we may call the *splittability* of an element $G \in \mathrm{Ext}(A, (G_a)^\nu)$, i.e. in whether or not G possesses a direct factor G_a, i.e. in whether or not G is indecomposable for *all* admissible vector group structures on $(G_a)^\nu$. Splittability can thus differ from decomposability only if $\nu > 1$ and we have characteristic $p \neq 0$. In this case, if we write $G = (G_a)^\nu B$ (with B abelian) and apply Prop. 4 (instead of 3) to the homomorphism $(G_a)^\nu \to G/B$, we get G splittable if and only if the α_1 of Prop. 4 is zero, i.e. if and only if the Lie algebra map corresponding to $(G_a)^\nu \to G/B$ is not trivial; thus G unsplittable for $\nu > 1$ means that the Lie algebra of $(G_a)^\nu$ is contained in that of B. In particular, if $\dim A > 1$ then the Γ of Prop. 11 is splittable except when all the above c_{ij} are zero, a very special case since it implies $B \cap H = 0$, and hence that A possesses only one point of order p.

Let C be a complete nonsingular curve. For the convenience of the reader, we give a brief account of the cohomology group $H^1(C, \mathcal{O}_C)$. Any element of this group is determined by an open covering $\{U_i\}_{i \in I}$ of C and a subset $\{f_{ij}\}_{i,j \in I}$ of $\Omega(C)$ (Ω being the universal domain) such that each f_{ij} is everywhere finite on $U_i \cap U_j$ and $f_{jk} - f_{ik} + f_{ij} = 0$ for all $i, j, k \in I$. Thus we can find $\{f_i\}_{i \in I}$ such that $f_{ij} = f_j - f_i$, and conversely, any set $\{U_i, f_i\}_{i \in I}$, where $\{U_i\}$ is an open covering of C, $\{f_i\} \subset \Omega(C)$, and each $f_j - f_i$ is without poles on $U_i \cap U_j$, will produce an element of $H^1(C, \mathcal{O}_C)$. To such a set $\{U_i, f_i\}$ associate a repartition $\{\tau_P\}_{P \in C}$ of $\Omega(C)$ (cf. [4]) such that $f_i - \tau_P$ is finite at P whenever $P \in U_i$. Denoting by $\Omega(C)^*$ the vector space of repartitions of C and, for any divisor $\mathfrak{A}$ of C, by $\mathcal{L}^*(\mathfrak{A})$ the subspace consisting of repartitions that are everywhere locally multiples of $-\mathfrak{A}$, we map $\{\tau_P\}$ canonically into $\Omega(C)^*/\mathcal{L}^*(0) + \Omega(C)$. One verifies directly that the resulting map $H^1(C, \mathcal{O}_C) \to \Omega(C)^*/\mathcal{L}^*(0) + \Omega(C)$ is well-defined and an Ω-linear bijection. If the genus of C is g, we deduce that $\dim H^1(C, \mathcal{O}_C) = g$. Furthermore, if $P_1, \cdots, P_g$ are distinct points of C such that the divisor $P_1 + \cdots + P_g$ is nonspecial (such points can always be found), then $\Omega(C)^* = \mathcal{L}^*(P_1 + \cdots + P_g) + \Omega(C)$, so that a basis of $H^1(C, \mathcal{O}_C)$ can be obtained from g repartitions the i-th of which ($i = 1, \cdots, g$) is everywhere finite except for a simple pole at P_i.

THEOREM 2. *Let C be a complete nonsingular curve and $\phi: C \to J$ the canonical map of C into its jacobian variety. Then the associated cohomology map*

$$\phi^*: H^1(J, \mathcal{O}_J) \to H^1(C, \mathcal{O}_C)$$

is bijective.

By Th. 1, the canonical map $\mathrm{Ext}(J, G_a) \to H^1(J, \mathcal{O}_J)$ is bijective, so we need to prove bijectivity for the composed map $\mathrm{Ext}(J, G_a) \to H^1(C, \mathcal{O}_C)$. But if g is the genus of C, then $\dim H^1(C, \mathcal{O}_C) = g$ and $\dim \mathrm{Ext}(J, G_a) \leqq g$ (Prop. 11), so only surjectivity need be proved. We shall do this by showing that for any $P \in C$, there exists a $J' \in \mathrm{Ext}(J, G_a)$ which produces an element of $H^1(C, \mathcal{O}_C)$ corresponding to a repartition of C that is everywhere finite except for a simple pole at P. Assume, as we may, that $g > 0$, let k be a field of definition for C, J, and ϕ over which P is rational, and let $\mathfrak{o}$ be the local subring of $k(C)$ consisting of all functions of the form

$$(\text{element of } k) + (\text{element of } k(C) \text{ of order} \geqq 2 \text{ at } P).$$

Let J' be the generalized jacobian variety of C corresponding to $\mathfrak{o}$, $\tau: J' \to J$ the natural homomorphism, and let $\phi': C \to J'$ be the canonical map, all defined

over k and with ϕ' normalized so that $\tau\phi' = \phi$ (cf. [9]). Fix an element $t \in k(C)$ of order 1 at P; then t is a basis for $\bar{\mathfrak{o}}/\mathfrak{o}$ ($\bar{\mathfrak{o}}$ being the integral closure of $\mathfrak{o}$ in $k(C)$) and the map $a \to \phi'((1+at))$ (a constant) is a biregular isomorphism between G_a and the kernel of τ [9, Th. 11]. Thus we can consider $J' \in \mathrm{Ext}(J, G_a)$. The element of $H^1(C, \mathcal{O}_C)$ determined by J' is given by the G_a-principal fiber space $W = \tau^{-1}(\phi C)$. The map $\phi' : C \to J'$ gives a cross section of W that is regular except at P. To obtain a local cross section valid in a neighborhood of P, first note that if x is a quantity that is transcendental over k, then the divisor $(t)_x$ of C is rational over $k(x)$ and any k-specialization $x \to c$ admits a unique extension to a k-specialization $(x, (t)_x) \to (c, (t)_c)$. Hence if p is generic for C over k, the positive divisor $(t)_{t(p)} - p$ specializes uniquely to $(t)_0 - P$ over the k-specialization $p \to P$. Now define a rational map $\psi : C \to J'$, defined over k, by the rule

$$\psi p = \phi'(p - (t - t(p))) \qquad (= \phi'(p - (t)_{t(p)} + (t)_\infty)).$$

Since the divisors $(t)_\infty$ and $(t)_0 - P$ are both independent of P, we deduce that the k-specialization $p \to P$ can be extended to a specialization of ψp into some point of J'. Thus ψ, which is clearly a rational cross section of W, is regular on an open neighborhood U_1 of P. The fiber space W is thus determined by the open covering of C by $U_0 = C - P$ and U_1 and the single transition function $f_{01} = \psi - \phi'$. But

$$\psi p - \phi' p = \phi'(-(t - t(p))) = -\phi'((1 - t/t(p))) = 1/t(p) \in G_a.$$

This cohomology class is represented by the repartition of C that is $1/t$ at P and 0 elsewhere, which completes the proof.

Note that the above cohomology map ϕ^* remains unchanged if ϕ is altered by a constant translation on J; this is clear from the proof, and also follows from the Lemma to Th. 1.

LEMMA 1. *Any abelian variety is the image of a direct product of jacobian varieties under a separable rational homomorphism.*

For any variety V of dimension > 0, simple point $P \in V$, and tangent vector τ to V at P, one can find a curve $C \subset V$ that has a simple point at P and is tangent to τ: it suffices to take V to be a variety in affine space and then intersect it with a suitably general linear subspace of the correct dimension passing through P and τ. Given the abelian variety A, find curves $C_1, \cdots, C_n$ on A that have simple points at 0 and whose tangent spaces there span the tangent space to A at 0. Consider the canonical map $C_i \to J_i$ of each C_i into its jacobian variety. The injection $C_i \to A$ factors into $C_i \to J_i \to A$, each map $J_i \to A$ being a rational homomorphism. Hence

we have a rational homomorphism from $J_1 \times \cdots \times J_n$ into A whose corresponding Lie algebra map is surjective. This last homomorphism is thus both surjective and separable.

LEMMA 2. *If H is a finite commutative group, then the vector spaces* $\mathrm{Hom}(H, G_a)$ *and* $\mathrm{Ext}(H, G_a)$ *have a common dimension, this being zero in the case of characteristic zero and the number of generators of H/pH if the characteristic is $p \neq 0$.*

We may assume H to be cyclic of order q^n, where q is prime and $n > 0$. If q is not the field characteristic, then $\mathrm{Hom}(H, G_a) = 0$ since G_a has no element of order q^n, and $\mathrm{Ext}(H, G_a) = 0$ since G_a is divisible by q^n. So let q equal the field characteristic $p \neq 0$ and let t be a fixed generator of H. Each element of $\mathrm{Hom}(H, G_a)$ is determined by the image of t in G_a, so $\dim \mathrm{Hom}(H, G_a) = 1$. On the other hand, if $G \in \mathrm{Ext}(H, G_a)$ and $t' \in G$ is in the inverse image of t, we have $p^n t' \in G_a$, and $p^n t'$ does not depend on the choice of t'. One verifies directly that the map $\mathrm{Ext}(H, G_a) \to G_a$ defined by $G \to p^n t'$ is a vector space isomorphism, so $\dim \mathrm{Ext}(H, G_a) = 1$.

THEOREM 3. *For any abelian variety A,* $\dim \mathrm{Ext}(A, G_a) = \dim A$.

We already know that $\dim \mathrm{Ext}(A, G_a) \leqq \dim A$ (Prop. 11) with equality holding in the case of jacobian varieties (Th. 2), hence also for direct products of jacobians (Prop. 5, Cor.). Using Lemma 1, we are reduced to showing that if A is an abelian variety for which the theorem holds and B an algebraic subgroup of A, then the theorem also holds for A/B. Such being the case, Prop. 6 gives the exact sequence

$$\mathrm{Hom}(A, G_a) \to \mathrm{Hom}(B, G_a) \to \mathrm{Ext}(A/B, G_a) \to \mathrm{Ext}(A, G_a) \to \mathrm{Ext}(B, G_a).$$

But $\mathrm{Hom}(A, G_a) = 0$, so

$$\dim \mathrm{Ext}(B, G_a) - \dim \mathrm{Ext}(A, G_a) + \dim \mathrm{Ext}(A/B, G_a) - \dim \mathrm{Hom}(B, G_a) \geqq 0.$$

Now the component of the identity B_0 of B is an abelian variety, hence divisible, so we can write $B = B_0 \times H$, where H is a finite group. Since $\dim \mathrm{Ext}(B, G_a) = \dim \mathrm{Ext}(B_0, G_a) + \dim \mathrm{Ext}(H, G_a)$ and $\dim \mathrm{Hom}(B, G_a) = \dim \mathrm{Hom}(B_0, G_a) + \dim \mathrm{Hom}(H, G_a) = \dim \mathrm{Hom}(H, G_a)$, Lemma 2 implies

$$\dim \mathrm{Ext}(B_0, G_a) - \dim \mathrm{Ext}(A, G_a) + \dim \mathrm{Ext}(A/B, G_a) \geqq 0.$$

But $\dim \mathrm{Ext}(B_0, G_a) \leqq \dim B_0$, $\dim \mathrm{Ext}(A/B, G_a) \leqq \dim A/B$, and we have assumed that $\dim \mathrm{Ext}(A, G_a) = \dim A$. The fact that $\dim A = \dim A/B + \dim B_0$ implies that all inequality signs above are actually equalities.

COROLLARY. *If B is an algebraic subgroup of the abelian variety A, we have a natural exact sequence*

$$0 \to \mathrm{Hom}(B, G_a) \to \mathrm{Ext}(A/B, G_a) \to \mathrm{Ext}(A, G_a) \to \mathrm{Ext}(B, G_a) \to 0.$$

Appendix.

We shall use freely the conventions of [6] and [9], together with certain results in [4].

LEMMA. *Let K be an algebraic function field of one variable that is separably generated over its constant field k, $\mathfrak{o}$ a semilocal subring of K, and ω a differential of K. Then ω is an $\mathfrak{o}$-differential of first kind if, whenever $z \in \mathfrak{o}$ is a separating variable for K/k, we have* $\mathrm{Sp}_{K/k(z)}\omega = 0$.

Letting ω, z be as above, for any repartition τ of $k(z)$ (hence also of K), we have $(\mathrm{Sp}_{K/k(z)}\omega)(\tau) = \omega(\tau) = \sum_P \mathrm{res}_P \tau\omega$, P ranging over all prime divisors of K/k. Thus $\sum_P \mathrm{res}_P \tau\omega = 0$ for all repartitions τ of $k(z)$. In particular, for any prime divisor p of $k(z)/k$ we have $\sum_{P \to p} \mathrm{res}_P z\omega = 0$. Suppose first that ω has a pole at a prime divisor Q that is prime to the places of $\mathfrak{o}$. Then there exists an element $t \in K$ such that $v_Q(t) \geqq 0$ and $\mathrm{res}_Q t\omega \neq 0$. Fix an element $a \in k$ that is distinct from $Q(t)$, a separating variable z_0 of K/k, and an integer n greater than the order of any pole of ω and so large that any element of K of order $\geqq n$ at each place of $\mathfrak{o}$ is in $\mathfrak{o}$. Choose $z \in K$ so that

(1) $v_Q(t - z) \geqq n$.

(2) $v_P(z - a) \geqq n$ if P is a prime divisor of $\mathfrak{o}$.

(3) $v_P(z) \geqq n$ if P is a pole of ω distinct from Q and prime to the places of $\mathfrak{o}$.

(4) $v_{P_0}(z - z_0) > 1$ for some place P_0 of K that is not a zero of dz_0.

By (4), $dz - dz_0$ has a zero at P_0, so $dz_0 \neq 0$ implies $dz \neq 0$, i.e. z is a separating variable for K/k. By (2), $z \in \mathfrak{o}$. If q is the prime divisor of $k(z)$ lying under Q and $P \neq Q$ a prime divisor of K lying over q, then (using the same letters P, Q, q to represent places) $P(z) = Q(z) = Q(t) \neq a, \infty$; by (2), we get P prime to the places of $\mathfrak{o}$ and by (3), $v_P(z\omega) \geqq 0$. Thus $\sum_{P \to q} \mathrm{res}_P z\omega = \mathrm{res}_Q z\omega = \mathrm{res}_Q t\omega \neq 0$, a contradiction; hence we can have poles only at the places of $\mathfrak{o}$. Thus for any $z \in \mathfrak{o}$ that is a separating variable for K/k, we have $\sum_P \mathrm{res}_P z\omega = 0$, P now ranging over the prime divisors of $\mathfrak{o}$. But if we add to any nonseparating variable a separating

variable, we get a separating variable, so the last equation holds for all $z \in \mathfrak{o}$, precisely the condition that ω be an $\mathfrak{o}$-differential [6, Th. 8].

Remark. Even if K is not separably generated over k, a sufficient condition that ω be an $\mathfrak{o}$-differential of first kind is that $\mathrm{Sp}_{K/k(z)}\omega = 0$ for all $z \in \mathfrak{o}$ (the trace being understood to be zero if $z \in k$); this is shown by eliminating all mention of separating variables in the above proof. Conversely, if ω is an $\mathfrak{o}$-differential of first kind and $z \in \mathfrak{o}$ then we always have $\mathrm{Sp}_{K/k(z)}\omega = 0$: this is part of the Lemma to Th. 1 of [9].

In the case where the universal domain is the field of complex numbers, the following result has been proved transcendentally in [9, § 1].

PROPOSITION 12. *Let C be a complete nonsingular curve, $\mathfrak{o}$ a semilocal subring of functions on C, $\phi: C \to J$ the corresponding canonical map of C into its generalized jacobian variety. Then the associated map $\omega \to \phi^*\omega$ of differentials on J into differentials on C is an isomorphism between the space of invariant differentials of degree one on J and the space of $\mathfrak{o}$-differentials of first kind on C.*

We may assume that the $\mathfrak{o}$-genus π of C is > 0, for otherwise this is trivial. Let ω be an invariant differential on J and let k be an algebraically closed field of definition for C, the equivalence relation on C, J, ϕ, and ω. Let $z \in \mathfrak{o} \cap k(C)$ be a separating variable for $k(C)/k$ and write $k(C) = k(z, u)$, where $u \in k(C)$ is separably algebraic over $k(z)$. Let x be a quantity that is transcendental over k and write the divisor $(z - x)$ irredundantly as $P_1 + \cdots + P_n - Q_1 - \cdots - Q_n$. $z(P_i) = x$, $i = 1, \cdots, n$, so each P_i is generic for C over k; also each Q_i is a pole of z, hence rational over k. Since $z - x$ is a unit in $\mathfrak{o}$ we have $\phi P_1 + \cdots + \phi P_n = \phi Q_1 + \cdots + \phi Q_n$. By the last result of [13], for any point p that is rational over $k(P_1, \cdots, P_n)$, we have a differential $\omega(p)$ of $k(P_1, \cdots, P_n)/k$, and our last equation gives $\omega(\phi P_1) + \cdots + \omega(\phi P_n) = \omega(\phi Q_1) + \cdots + \omega(\phi Q_n)$. But for any $i = 1, \cdots, n$, we have $\omega(\phi P_i) = (\phi^*\omega)(P_i)$ and $\omega(\phi Q_i) = 0$, so $(\phi^*\omega)(P_1) + \cdots + (\phi^*\omega)(P_n) = 0$. For each $i = 1, \cdots, n$, $k(P_i) = k(z(P_i), u(P_i)) = k(x, u(P_i))$, so each P_i, hence also $k(P_1, \cdots, P_n)$ is separably algebraic over $k(x)$; furthermore, $P_1, \cdots, P_n$ is a complete set of conjugates over $k(x)$. Write $\phi^*\omega = y\,dz$, where $y \in k(C) = k(z, u)$. Then for $i = 1, \cdots, n$ we have $(\phi^*\omega)(P_i) = y(P_i)\,dz(P_i) = y(P_i)\,dx$, so $y(P_1)\,dx + \cdots + y(P_n)\,dx = 0$, i.e. $\mathrm{Sp}_{k(P_1)/k(x)} y(P_1)\,dx = 0$. In other words, $\mathrm{Sp}_{k(C)/k(z)}\phi^*\omega = 0$, proving that $\phi^*\omega$ is an $\mathfrak{o}$-differential of first kind. Now consider the sequence of rational maps $C^\pi \to C^{(\pi)} \to J$ (C^π and $C^{(\pi)}$ being the direct and symmetric products,

respectively) given by $p_1 \times \cdots \times p_\pi \to p_1 + \cdots + p_\pi \to \phi p_1 + \cdots + \phi p_\pi$. For $p_1, \cdots, p_\pi$ independent generic points of C over k, we have

$$\omega(\phi p_1 + \cdots + \phi p_\pi) = \omega(\phi p_1) + \cdots + \omega(\phi p_\pi)$$
$$= (\phi^*\omega)(p_1) + \cdots + (\phi^*\omega)(p_\pi).$$

Since the map $C^\pi \to J$ is generically surjective and separable, $\omega \neq 0$ implies $\phi^*\omega \neq 0$. We are through, since both vector spaces in the proposition have dimension π.

PROPOSITION 13. *Let C be a complete nonsingular curve, $\mathfrak{o}$ a semilocal subring of functions on C, J the corresponding generalized jacobian variety. Then the maximal connected linear algebraic subgroup of J is a direct product of G_a's if and only if each $\mathfrak{o}$-differential of first kind on C is a differential of second kind.*

The maximal connected linear algebraic subgroup H of J is the kernel of the natural homomorphism from J to the ordinary jacobian variety of C, hence is isomorphic to the multiplicative group of units of $\bar{\mathfrak{o}}$ modulo units of $\mathfrak{o}$, $\bar{\mathfrak{o}}$ being the integral closure of $\mathfrak{o}$. By Prop. 2, H is a product of G_a's if and only if all its elements are of order p if the characteristic is $p \neq 0$, while no element $\neq 0$ is of finite order if the characteristic is zero. If $\mathfrak{o} = \mathfrak{o}_1 \cap \mathfrak{o}_2$, where $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are semilocal subrings of functions on C with no common place, then $\bar{\mathfrak{o}} = \bar{\mathfrak{o}}_1 \cap \bar{\mathfrak{o}}_2$ and H decomposes into a direct product in the obvious way. Furthermore, the $\mathfrak{o}$-differentials of first kind are precisely the sums of $\mathfrak{o}_1$-differentials of first kind and $\mathfrak{o}_2$-differentials of first kind [6, Th. 8, Cor. 3], so it suffices to prove the proposition for $\mathfrak{o}_1$ and $\mathfrak{o}_2$ instead of $\mathfrak{o}$. Hence we may assume that $\mathfrak{o}$ is a local ring. If P, Q are distinct places of $\mathfrak{o}$, then any function on C that is very near 1 at P and very near some root of unity distinct from 1 at Q will be a unit in $\bar{\mathfrak{o}}$ some power of which is in $\mathfrak{o}$, so H will not be a product of G_a's. In this case, a differential of third kind with simple poles at P and Q and no poles elsewhere will be an $\mathfrak{o}$-differential of first kind and not of second kind. Thus we may assume that $\mathfrak{o}$ has a single place P. In characteristic zero, any $\mathfrak{o}$-differential of first kind will have zero residue at P and no poles elsewhere, hence be of second kind, while H will be a product of G_a's [9, Th. 11, Cor.]. In characteristic $p \neq 0$, the condition that H be a product of G_a's is that $f^p \in \mathfrak{o}$ for each $f \in \bar{\mathfrak{o}}$, a condition equivalent to having $\operatorname{res}_P f^p\omega = 0$ for each $f \in \bar{\mathfrak{o}}$ and each $\mathfrak{o}$-differential ω of first kind [6, Th. 8, Cor. 1]. But this is (trivially, cf. [7, Lemma 7]) equivalent to each such ω being of second kind.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] I. Barsotti, "Factor systems and differentials on abelian varieties," *Transactions of the American Mathematical Society*, vol. 84 (1957).

[2] ———, "Abelian varieties over fields of positive characteristic," *Rendiconti del Circolo Matematico di Palermo*, Series II, vol. 5 (1956).

[3] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956).

[4] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, American Mathematical Society, New York, 1951.

[5] F. Hirzebruch, *Neue Topologische Methoden in der Algebraischen Geometrie*, Berlin, 1956.

[6] M. Rosenlicht, "Equivalence relations on algebraic curves," *Annals of Mathematics*, vol. 56 (1952).

[7] ———, "Differentials of the second kind for algebraic function fields of one variable," *Annals of Mathematics*, vol. 57 (1953).

[8] ———, "Simple differentials of second kind on Hodge manifolds," *American Journal of Mathematics*, vol. 75 (1953).

[9] ———, "Generalized jacobian varieties," *Annals of Mathematics*, vol. 59 (1954).

[10] ———, "Commutative algebraic group varieties," *Algebraic Geometry and Topology, A Symposium in Honor of S. Lefschetz*, Princeton, 1957.

[11] ———, "Group varieties and differential forms," *Proceedings of the International Congress of Mathematicians* 1954, vol. III, Amsterdam, 1956.

[12] ———, "Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956).

[13] ———, "A note on derivations and differentials on algebraic varieties," *Portugaliae Mathematica*, vol. 16 (1957).

[14] ———, "Some rationality questions on algebraic groups," *Annali di Matematica Pura ed Applicata*, Series IV, vol. 43 (1957).

[15] J-P. Serre, "Faisceaux algébriques cohérents," *Annals of Mathematics*, vol. 61 (1955).

[16] ———, *Groupes Algébriques et Théorie du Corps de Classes*, mimeographed notes of course at Collège de France, 1957.

[17] A. Weil, *Foundations of Algebraic Geometry*, Colloquium Publications of the American Mathematical Society, New York, 1946.

[18] ———, *Variétés Abéliennes et Courbes Algébriques*, Paris, 1948.

[19] ———, *Fibre-Spaces in Algebraic Geometry*, mimeographed notes by A. Wallace of course at University of Chicago, 1952.

[20] ———, "On the projective embedding of abelian varieties," *Algebraic Geometry and Topology, A Symposium in Honor of S. Lefschetz*, Princeton, 1957.

[21] ———, "On algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955).

[22] ———, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955).

QUELQUES PROPRIÉTÉS DES VARIÉTÉS ABÉLIENNES EN CARACTÉRISTIQUE p.*

par JEAN-PIERRE SERRE.

à Emil Artin.

Introduction. Soit A une variété abélienne de dimension g, définie sur un corps algébriquement clos k. Lorsque $k = \mathbf{C}$, la variété A est un tore complexe, ce qui montre que l'algèbre de cohomologie $H^*(A, \mathbf{C})$ est une algèbre extérieure engendrée par $2g$ éléments de degré 1, et que l'on a $h^{r,s}(A) = \binom{g}{r} \cdot \binom{g}{s}$. On peut se demander si ces résultats cohomologiques restent valables en caractéristique $p > 0$; ils gardent un sens, à cause de leur transcription en termes de faisceaux cohérents, cf. [20]. La première question qui se posait était la détermination de $h^{0,1}(A) = \dim. H^1(A, \mathcal{O}_A)$; elle vient d'être résolue par Rosenlicht [19]. Rosenlicht montre d'abord (*loc. cit.*, Th. 1) que $H^1(A, \mathcal{O}_A)$ est isomorphe au groupe $\mathrm{Ext}(A, G_a)$ des classes d'extensions de A par le groupe additif G_a, et il prouve ensuite (*ibid.*, Th. 3) que $\mathrm{Ext}(A, G_a)$ est un k-espace vectoriel de dimension g; ce dernier résultat a été également obtenu par Barsotti [3].

De là, on passe facilement à la détermination complète de $H^*(A, \mathcal{O}_A)$, et on montre qu'une variété abélienne *n'a pas de torsion homologique* (au sens de [22]) ; c'est ce qui est fait au § 1. Ce § contient également un exemple de variété abélienne A dont le second groupe de cohomologie à valeurs dans les vecteurs de Witt (le groupe $H^2(A, \mathcal{W})$) *n'est pas* un module de type fini, contrairement à ce que j'avais imprudemment conjecturé dans [22]. Cet exemple n'est guère encourageant du point de vue "définition homologique des nombres de Betti"!

Le § 2 est consacré à la classification des *isogénies radicielles de hauteur* 1. On sait que les isogénies séparables $A \to A'$ correspondent aux sous-groupes finis de A; une correspondance analogue vaut pour les isogénies radicielles de hauteur 1, à condition de remplacer les sous-groupes finis de A par certaines sous-algèbres de l'algèbre de Lie de A (cf. nº. 5, Th. 3). Ce résultat n'est d'ailleurs pas nouveau: il est contenu (au moins dans le cas commutatif) dans le mémoire de Barsotti cité plus haut. Barsotti considère même des

* Received January 30, 1958.

isogénies de hauteur quelconque, et les classifie au moyen de la théorie de Dieudonné; ses énoncés, plus complets, sont peut-être moins maniables; c'est pourquoi j'ai cru utile de reprendre le cas de la hauteur 1, en m'appuyant uniquement sur la "théorie de Galois" de Jacobson [14]. D'ailleurs, beaucoup de questions sur les isogénies radicielles se laissent facilement ramener au cas de la hauteur 1 (cf. § 3, Lemme 9). Le § 2 se termine par une application à un théorème d'Igusa [12].

Nous rappelons au début du § 3 les principales propriétés élémentaires des groupes $\mathrm{Ext}(A,B)$ (cf. aussi [19]), et nous indiquons le comportement de ces groupes lorsque l'on effectue sur A une isogénie radicielle de hauteur 1. On en déduit une nouvelle démonstration du théorème de Barsotti [3] suivant lequel une variété abélienne *n'a pas de torsion* (dans le groupe de Néron-Severi). Le reste du § 3 est consacré à montrer que la représentation des endomorphismes de A dans $H^1(A,\mathfrak{M})$, augmentée de celle dans les points d'ordre p^ν de la variété duale, est l'analogue p-adique des représentations l-adiques de Weil (voir Th. 6 et Th. 7).[1]

§ 1. Cohomologie des variétés abéliennes.

1. Structure de l'algèbre $H^*(A)$. Soit A une variété abélienne de dimension g, définie sur un corps algébriquement clos k, et soit $\mathfrak{O}_A$ le faisceau de ses anneaux locaux. Posons $H^*(A)=\sum_0^\infty H^n(A,\mathfrak{O}_A)$; l'opération de *cup-produit* munit l'espace vectoriel $H^*(A)$ d'une structure d'algèbre graduée; du fait que la multiplication dans $\mathfrak{O}_A$ est associative et commutative, celle de $H^*(A)$ est associative et anticommutative (pour toutes les propriétés du cup-produit, nous renvoyons à l'ouvrage de Godement sur les faisceaux, [8], Chap. II, § 6).

Ce qui précède n'utilise que la structure de variété algébrique de A; utilisons maintenant sa loi de composition $s: A\times A\to A$. Par passage à la cohomologie, elle définit un homomorphisme $s^*: H^*(A)\to H^*(A\times A)$.

Mais la *formule de Künneth* s'applique au faisceau des anneaux locaux (et plus généralement à des faisceaux cohérents quelconques): cela se voit, par exemple, en appliquant le théorème d'Eilenberg-Zilber ([8], Chap. I, Th. 3.10.1) aux complexes obtenus à partir de recouvrements affines. On a donc $H^*(A\times A)=H^*(A)\otimes H^*(A)$. De plus, le fait que A ait un élément neutre pour s montre, comme dans le cas classique, que, si $\deg(x)>0$, on a

[1] P. Cartier a également obtenu une telle représentation (non publié); sa méthode est différente: il utilise le "module de Dieudonné" de la variété duale de A à la place de $H^1(A,\mathfrak{w})$.

$s^*(x) = x \otimes 1 + 1 \otimes x + \sum y_i \otimes z_i$, avec $\deg(y_i) > 0$, $\deg(z_i) > 0$. Cela signifie que $H^*(A)$ est une *algèbre de Hopf* au sens de Borel [4], § 6. Or on a:

LEMME 1. *Soit $H = \sum_0^\infty H^n$ une algèbre de Hopf sur k, associative, anticommutative, et connexe (i.e. $H^0 = k$). Soit g un entier tel que $H^n = 0$ pour $n > g$. On a alors* $\dim. H^1 \leqq g$, *et, si l'égalité est vérifiée, l'algèbre H s'identifie à l'algèbre extérieure du k-espace vectoriel H^1.*

D'après le théorème de structure de Borel (*loc. cit.*, Th. 6.1), l'algèbre H est produit tensoriel sur k d'algèbres monogènes $k[x_i]$. Posons $n_i = \deg(x_i)$. Le produit de tous les x_i est un élément non nul de H, de degré égal à $\sum n_i$, d'où $\sum n_i \leqq g$. En particulier, le nombre des x_i de degré 1 est $\leqq g$; comme ce nombre est visiblement égal à $\dim. H^1$, ceci démontre l'inégalité $\dim. H^1 \leqq g$. S'il y a égalité, tous les x_i sont nécessairement de degré 1; de plus leurs carrés sont nuls, car, si l'on avait ${x_1}^2 \neq 0$, le produit ${x_1}^2 \otimes x_2 \otimes \cdots \otimes x_g$ serait un élément non nul de H, de degré $g+1$, ce qui est impossible. L'algèbre H s'identifie donc bien à l'algèbre extérieure sur H^1.

Les hypothèses du lemme précédent sont vérifiées par l'algèbre de Hopf $H = H^*(A)$: on a $H^0(A) = k$ puisque A est connexe et complète, et $H^n = 0$ pour $n > g$ puisque A est de dimension g ([21], Th. 2, ou même [20], n°. 66, Th. 1 si l'on tient compte du fait qu'une variété abélienne admet un plongement projectif). On a donc l'inégalité $\dim. H^1(A, \mathcal{O}_A) \leqq g$; on notera que Rosenlicht, dans sa démonstration de *l'égalité* $\dim. H^1(A, \mathcal{O}_A) = g$ ([19], Th. 3) a d'abord besoin d'établir l'inégalité précédente (*loc. cit.*, Lemme 3). Si l'on fait maintenant usage de l'égalité en question, on obtient:

THÉORÈME 1. *Soient A une variété abélienne de dimension g, et $\mathcal{O}_A$ le faisceau de ses anneaux locaux. L'algèbre de cohomologie*

$$H^*(A) = \sum H^n(A, \mathcal{O}_A)$$

s'identifie à l'algèbre extérieure de l'espace vectoriel $H^1(A, \mathcal{O}_A)$, qui est de dimension g.

Soit Ω^r le faisceau des formes différentielles régulières de degré r sur A, et posons $h^{r,s} = \dim. H^s(A, \Omega^r)$. Du fait que le fibré tangent à une variété de groupe est trivial, le faisceau Ω^r est isomorphe à la somme directe de $\binom{g}{r}$ copies du faisceau $\mathcal{O}_A$, et l'on en déduit $h^{r,s} = \binom{g}{r} \cdot \binom{g}{s}$.

On voit en particulier que la *formule de symétrie* $h^{r,s} = h^{s,r}$ est valable pour les variétés abéliennes.

2. Absence de torsion homologique sur les variétés abéliennes. Supposons que la caractéristique p du corps de base soit >0. On sait ([22], n°. 3) que l'on peut associer à toute variété algébrique X des *opérations de Bockstein*, opérant sur $H^*(X, \mathcal{O}_X)$; on dit que X *n'a pas de torsion homologique* si ces opérations sont identiquement nulles.

THÉORÈME 2. *Une variété abélienne n'a pas de torsion homologique.*

Soit A une variété abélienne, et soient $\beta_1, \cdots, \beta_n, \cdots$ les opérations de Bockstein associées à A. Supposons démontré que $\beta_i = 0$ pour $i < n$, et montrons que $\beta_n = 0$. Comme β_n opère sur l'algèbre de cohomologie de β_{n-1} (*loc. cit.*), on voit que, dans le cas présent, β_n opère sur $H^*(A)$. De plus β_n vérifie la formule de dérivation suivante (*loc. cit.*, formule (8)) :

$$\beta_n(x \cdot y) = \beta_n(x) \cdot F^n(y) + (-1)^{\deg(x)} F^n(x) \cdot \beta_n(y), \qquad x, y \in H^*(A),$$

où F désigne l'opération définie par la puissance p-ème sur $\mathcal{O}_A$.

Puisque, en vertu du Th. 1, $H^*(A)$ est engendrée par ses éléments de degré 1, il nous suffira donc de montrer que $\beta_n(x) = 0$ si $x \in H^1(A)$. Dans ce cas, on a évidemment $s^*(x) = x \otimes 1 + 1 \otimes x$, autrement dit l'élément x est un élément *primitif* de l'algèbre de Hopf $H^*(A)$. Si l'on pose $y = \beta_n(x)$, on a $y \in H^2(A)$; de plus, en vertu du caractère fonctoriel de β_n, on a :

$$s^*(y) = s^*\beta_n(x) = \beta_n s^*(x) = \beta_n(x \otimes 1 + 1 \otimes x) = y \otimes 1 + 1 \otimes y.$$

L'élément y est donc un élément primitif de $H^*(A)$, de degré 2. Pour prouver que $y = 0$, il suffit alors d'établir le lemme suivant :

LEMME 2. *Les seuls éléments primitifs non nuls de $H^*(A)$ sont de degré 1.*

Soit $V = H^1(A)$; d'après le Théorème 1, on a $H^*(A) = \wedge V$. L'homomorphisme $s^* : H^*(A) \to H^*(A) \otimes H^*(A)$ s'identifie donc à l'application "diagonale" $\delta : \wedge V \to \wedge V \otimes \wedge V = \wedge(V + V)$.

On est alors ramené à démontrer qu'aucun élément non nul $y \in \wedge V$, de degré $\geqq 2$, ne vérifie l'identité $\delta(y) = y \otimes 1 + 1 \otimes y$. C'est là un simple exercice d'algèbre extérieure ; on peut, par exemple, considérer la composante $\lambda(y)$ de $\delta(y)$ dans $\wedge V \otimes V$, et la "contracter" avec un élément v' du dual V' de V ; on obtient ainsi un élément de $\wedge V$ qui n'est autre que le *produit intérieur* de y par v' ; par hypothèse, on a $\lambda(y) = 0$, ce qui montre le produit intérieur de y par tout élément de V' est nul, d'où $y = 0$, comme on sait.

3. Un contre-exemple. Soit X une variété projective, et soit $\mathscr{W}_n$ le faisceaux des *vecteurs de Witt* de longueur n à coefficients dans le faisceau $\mathscr{O}_X$ des anneaux locaux de X (cf. [22], § 1). Si q est un entier $\geqq 0$, le groupe $H^q(X, \mathscr{W}_n)$ est muni de façon naturelle d'une structure de Λ-module, Λ désignant l'anneau $W(k)$ des vecteurs de Witt de longueur infinie sur le corps de base k. Lorsque n varie, les $H^q(X, \mathscr{W}_n)$ forment un système projectif, dont la limite est notée $H^q(X, \mathscr{W})$; c'est un Λ-module. Si $q = 0$, ou, si $q = 1$ et si X est normale, on sait (*loc. cit.*, Prop. 4) que $H^q(X, \mathscr{W})$ est un Λ-module *de type fini*; nous allons montrer que ce résultat *n'est plus valable pour* $q = 2$, *même si l'on suppose* X *non singulière.*

Nous prendrons pour X une variété abélienne de dimension 2, telle que l'endomorphisme $F: H^1(X, \mathscr{O}_X) \to H^1(X, \mathscr{O}_X)$ soit nul, par exemple le produit de deux courbes elliptiques dont l'invariant de Hasse est nul (cf. [9] ainsi que [22], § 2).

LEMME 3. *Pour tout* $n \geqq 0$, *l'homomorphisme*

$$F: H^2(X, \mathscr{W}_n) \to H^2(X, \mathscr{W}_n)$$

est nul.

Posons, pour simplifier les notations, $H_n{}^q = H^q(X, \mathscr{W}_n)$; on a en particulier $H_1{}^q = H^q(X, \mathscr{O}_X)$. Du fait que X n'a pas de torsion homologique (Théorème 2), on a une suite exacte:

$$0 \to H_{n-1}{}^q \to H_n{}^q \to H_1{}^q \to 0.$$

où le premier homomorphisme est le "décalage" V, et le second l'opération de "restriction" itérée R^{n-1}; pour la définition précise et les propriétés des opérations F, V, R, nous renvoyons à [22], § 1.

Nous raisonnerons par récurrence sur n, le cas $n = 0$ étant trivial. Puisque F et V commutent, il s'ensuit que F est nul sur $V(H_{n-1}{}^2)$; de plus, en vertu du Th. 1, $H_1{}^2$ est un espace de dimension 1, ayant pour base le cup-produit de deux éléments $x, x' \in H_1{}^1$. Choisissons alors des éléments $y, y' \in H_n{}^1$ tels que $R^{n-1}y = x$, $R^{n-1}y' = x'$; le cup-produit $y \cdot y' \in H_n{}^2$ a un sens, puisque $\mathscr{W}_n$ est un faisceau d'anneaux, et l'image de $y \cdot y'$ par R^{n-1} est $x \cdot x'$; le Λ-module $H_n{}^2$ est donc engendré par $V(H_{n-1}{}^2)$ et par $y \cdot y'$, et il nous suffira de montrer que $F(y \cdot y') = 0$.

Vu l'hypothèse faite sur X, on a $Fx = Fx' = 0$ dans $H_1{}^1$; la suite exacte écrite ci-dessus montre alors qu'il existe $z, z' \in H_{n-1}{}^1$ avec $Fy = Vz$, $Fy' = Vz'$; comme $F(y \cdot y') = Fy \cdot Fy'$, on en déduit $F(y \cdot y') = Vz \cdot Vz'$. En appliquant

l'identité $Va \cdot b = V(a \cdot FRb)$, on voit que $Vz \cdot Vz' = V(z \cdot FRVz')$; mais $FRV = p$, et on obtient finalement :

$$F(y \cdot y') = Vz \cdot Vz' = V(p \cdot z \cdot z').$$

Le produit $z \cdot z'$ appartient à H^2_{n-1} ; d'après l'hypothèse de récurrence il est annulé par F, et *a fortiori* par $p = RVF$; on trouve donc bien $F(y \cdot y') = 0$, ce qui achève la démonstration.

COROLLAIRE. *Le* Λ*-module* $H^2(X, \mathcal{W}) = \lim. H^2(X, \mathcal{W}_n)$ *est annulé par* p*. et ce n'est pas un module de type fini sur* Λ.

Puisque F est nul sur chaque $H^2(X, \mathcal{W}_n)$, il est nul sur leur limite projective $H^2(X, \mathcal{W})$; comme $p = FV$ sur $H^2(X, \mathcal{W})$, on voit bien que p annule $H^2(X, \mathcal{W})$; du fait que $W(k)/p \cdot W(k) = k$, cela signifie que $H^2(X, \mathcal{W})$ est un k-espace vectoriel. Le même raisonnement vaut pour chacun des $H^2(X, \mathcal{W}_n)$; de plus, la suite exacte écrite ci-dessus montre que la dimension de $H^2(X, \mathcal{W}_n)$ est n ; la dimension de leur limite projective est donc infinie, cqfd.

§ 2. Isogénies radicielles de hauteur 1.

4. Résultats préliminaires. Soit G un groupe algébrique connexe, de dimension r, et soit $\mathfrak{t}(G)$ son *algèbre de Lie*, identifiée à l'espace vectoriel des champs de vecteurs tangents sur G, invariants à gauche. Soit K le corps des fonctions rationnelles sur G, et soit $\Delta(K)$ le K-espace vectoriel formé par les dérivations de K, ou, ce qui revient au même, par les champs de vecteurs tangents sur G ; on démontre, comme dans la théorie classique des groupes de Lie (cf. [2], § 5 et [18], par exemple) que $\Delta(K) = \mathfrak{t}(G) \otimes_k K$; de plus, $\mathfrak{t}(G)$ est stable par l'opération de *crochet* $(X, Y) \to [X, Y]$ et l'opération de *puissance p-ème* $X \to X^p$, c'est une p-algèbre de Lie restreinte au sens de Jacobson (cf. [10], [13]). On notera que G opère aussi par translations à droite sur $\Delta(K)$; ces opérations laissent stable le sous-espace $\mathfrak{t}(G)$ de $\Delta(K)$, définissant ainsi la *représentation adjointe* de G.

LEMME 4. *Soit* N *un* K*-sous-espace vectoriel de* $\Delta(K)$, *et soit* $\mathfrak{n} = N \cap \mathfrak{t}(G)$; *c'est un* k*-sous-espace vectoriel de* $\mathfrak{t}(G)$.

a) *Pour que* N *soit stable par les translations à gauche de* G, *il faut et il suffit que* $N = \mathfrak{n} \otimes_k K$.

b) *Supposons* a) *vérifié. Pour que* N *soit stable par les translations à droite de* G, *il faut et il suffit que* $\mathfrak{n}$ *soit stable par la représentation adjointe de* G.

c) *Supposons* a) *vérifié. Pour que N soit stable pour le crochet et la puissance p-ème, il faut et il suffit que* $\mathfrak{n}$ *le soit.*

a). Si $N = \mathfrak{n} \otimes_k K$, il est clair que N est stable par les translations à gauche (nous dirons aussi "invariant à gauche"). Supposons réciproquement que cette condition soit vérifiée, et soit e_i $(1 \leqq i \leqq r)$ une base de $\mathfrak{t}(G)$ sur k, donc aussi de $\Delta(K)$ sur K. Soit E le sous-corps de K attaché à N relativement à la base e_i (cf. Bourbaki, Alg. II, § 5, déf. 2); d'après le Corollaire à la Prop. 10, *loc. cit.*, le corps E est contenu dans le sous-corps de K formé des fonctions invariantes par translation à gauche, sous-corps qui n'est autre que k. En appliquant alors le Th. 2, *loc. cit.*, on en déduit bien que N est engendré par $\mathfrak{n}$, d'où $N = \mathfrak{n} \otimes_k K$.

b). est évident par transport de structure.

c). On sait que $\mathfrak{t}(G)$ est stable pour le crochet et la puissance p-ème; s'il en est de même pour N, il en est donc aussi de même pour $N \cap \mathfrak{t}(G) = \mathfrak{n}$. Inversement, supposons $\mathfrak{n}$ stable pour le crochet; la formule évidente:

$$[aX, bY] = ab[X, Y] + aX(b) \cdot Y - bY(a) \cdot X, \quad a, b \in K,\ X, Y \in \Delta(K),$$

montre que N est stable pour le crochet. Supposons en outre que $\mathfrak{n}$ soit stable pour la puissance p-ème, et utilisons la formule de Hochschild (cf. par exemple [7], Lemme 4):

$$(aX)^p = a^p X^p + (aX)^{p-1}(a) \cdot X, \qquad a \in K, \quad X \in \Delta(K).$$

En appliquant cette formule avec $X \in \mathfrak{n}$, on voit que $(aX)^p \in N$. Pour montrer que N est stable pour la puissance p-ème, il suffira donc de montrer que, si $X \in N$, $Y \in N$, $X^p \in N$, $Y^p \in N$, on a aussi $(X+Y)^p \in N$. Pour cela on utilise la formule de Jacobson (cf. [13]):

$$(X+Y)^p = X^p + Y^p + s(X, Y), \qquad X, Y \in \Delta(K),$$

où $s(X, Y)$ est un "alternant," c'est-à-dire un polynôme (explicitement déterminé par Jacobson) par rapport à l'opération de crochet. Dans le cas qui nous occupe, on sait que l'on a $s(X, Y) \in N$, puisque N est stable pour le crochet, et il en résulte bien que $(X+Y)^p \in N$, ce qui achève la démonstration.

Remarque. Si G est *commutatif*, la représentation adjointe est triviale, et le crochet est nul dans $\mathfrak{t}(G)$. On voit donc que les sous-espaces N de $\Delta(K)$ invariants par translation et stables pour le crochet et la puissance p-ème

correspondent bijectivement aux sous-espaces vectoriels $\mathfrak{n}$ de $\mathfrak{t}(G)$ stables pour la puissance p-ème.

5. Classification des isogénies radicielles de hauteur 1. Conservons les notations du n°. précédent, et soit $\phi : G \to G'$ un homomorphisme surjectif de G dans un autre groupe algébrique G'. Identifions les algèbres de Lie de G et de G', soient $\mathfrak{t}(G)$ et $\mathfrak{t}(G')$, avec les espaces tangents à l'élément neutre. L'application ϕ admet une application tangente $\mathfrak{t}(\phi) : \mathfrak{t}(G) \to \mathfrak{t}(G')$, dont nous désignerons le noyau par $\mathfrak{n}(\phi)$.

D'autre part, puisque ϕ est surjectif, le corps K' des fonctions rationnelles sur G' se plonge dans le corps K; nous désignerons par $N(\phi)$ le sous-espace de $\Delta(K)$ formé des dérivations qui s'annulent sur K'.

LEMME 5. *On a $N(\phi) = \mathfrak{n}(\phi) \otimes_k K$, et $\mathfrak{n}(\phi)$ est stable pour le crochet, la puissance p-ème, et la représentation adjointe de G.*

(Nous dirons que $\mathfrak{n}(\phi)$ est une *p-sous-algèbre de Lie* de $\mathfrak{t}(G)$, stable pour la représentation adjointe).

Il est clair que $N(\phi)$ est stable pour les translations à droite et à gauche, ainsi que pour le crochet et l'opération de puissance p-ème. D'après le Lemme 4, a), on a donc $N(\phi) = \mathfrak{n} \otimes_k K$, avec $\mathfrak{n} = N(\phi) \cap \mathfrak{t}(G)$. Si $X \in \mathfrak{n}$, le vecteur tangent à l'origine X_e déterminé par le champ de vecteurs X est évidemment dans le noyau de $\mathfrak{t}(\phi)$. Réciproquement, soit X un champ de vecteurs invariant à gauche, et tel que $X_e \in \mathfrak{n}(\phi)$; par translation, on voit que X appartient en tout point de G au noyau de l'application tangente à ϕ, ce qui signifie que X appartient à $N(\phi)$; on a donc $\mathfrak{n} = \mathfrak{n}(\phi)$. En appliquant le Lemme 4, b), c), on voit alors que $\mathfrak{n}(\phi)$ est une p-sous-algèbre de Lie stable pour la représentation adjointe.

(Noter que le fait que $\mathfrak{n}(\phi)$ est stable pour la représentation adjointe implique que $\mathfrak{n}(\phi)$ est un *idéal* de $\mathfrak{t}(G)$, sans qu'il y ait équivalence entre ces propriétés).

Nous dirons que $\phi : G \to G'$ est une *isogénie radicielle* si l'extension K/K' est radicielle, c'est-à-dire si K' contient K^{p^n} pour n assez grand. Il revient au même de dire que ϕ est *bijective*, vu les propriétés connues des revêtements. L'isogénie sera dite *de hauteur 1* si l'on a $K' \supset K^p$. Le corps K^p correspond à l'isogénie "de Frobenius" $G \to G^p$, où G^p désigne la variété déduite de G par l'automorphisme $x \to x^p$ du domaine universel (au point de vue de la théorie des faisceaux, la variété G^p peut être définie comme ayant les mêmes points et la même topologie de Zariski que G, et comme faisceau d'anneaux le

faisceau des puissances p-èmes de $\mathcal{O}_G$). Si $\phi: G \to G'$ est une isogénie de hauteur 1, on a donc une factorisation $G \xrightarrow{\phi} G' \to G^p$, et G' est *la normalisée de G^p dans l'extension K'/K^p* (pour les propriétés de la normalisation des variétés, voir par exemple [15], Chap. V, §§ 3, 4). La connaissance du corps K' détermine donc de manière unique l'isogénie ϕ, à un isomorphisme près, et tout revient à caractériser les corps K', avec $K \supset K' \supset K^p$, qui correspondent à des isogénies. On a tout d'abord:

LEMME 6. *Pour qu'un sous-corps K' de K, contenant K^p, corresponde à une isogénie, il faut et il suffit qu'il soit stable par les translations à gauche et à droite par les éléments de G.*

La nécessité est triviale, démontrons la suffisance. Soit G' la normalisée de G^p dans K'/K^p; tout revient à montrer que l'application $(x, y) \to xy^{-1}$ de $G \times G$ dans G définit par passage au quotient une application régulière $G' \times G' \to G'$, car on en déduira la loi de groupe de G'. Il suffit même de démontrer que $G' \times G' \to G'$ est une application rationnelle, en vertu des propriétés de la normalisation (cf. [15], Chap. V, § 3).

Nous noterons $K \circ K$ le corps des fonctions rationnelles de $G \times G$; c'est le corps des fractions de l'anneau d'intégrité $K \otimes_k K$; même chose pour $K' \circ K'$. Il nous faut démontrer que, si $f \in K'$, la fonction rationnelle $g(x, y) = f(xy^{-1})$ appartient à $K' \circ K'$. On a en tout cas $g \in K \circ K$, d'où:

$$g(x, y) = [\sum_{i=1}^{i=n} a_i(x) \otimes b_i(y)]/c(x, y), \quad \text{avec} \quad c \in K \otimes K.$$

Quitte à remplacer c par sa puissance p-ème, on peut supposer $c \in K' \otimes K'$; de plus, si l'on prend n minimum, les a_i et les b_i sont linéairement indépendants sur k. Soit U un ouvert non vide de G tel que les fonctions b_i soient régulières sur U, et que $c(x, y)$ soit une fonction rationnelle de x (non identique à ∞) pour tout $y \in U$. Les fonctions b_i sont linéairement indépendantes sur U, et il existe donc des points $y_1, \cdots, y_n \in U$ tels que la matrice $c_{ij} = b_i(y_j)$ soit inversible. Le système linéaire

$$c(x, y_j) \cdot f(xy_j^{-1}) = \sum_{i=1}^{i=n} c_{ij} a_i(x), \qquad j = 1, \cdots, n,$$

montre alors que les $a_i(x)$ sont combinaisons linéaires des fonctions $c(x, y_j) \cdot f(xy_j^{-1})$; puisque K' est invariant à droite, ces dernières fonctions appartiennent à K'. On a donc $a_i \in K'$ pour tout i, et de même $b_i \in K'$ pour tout i, cqfd.

Nous pouvons maintenant appliquer la *théorie de Jacobson* pour les extensions radicielles de hauteur 1 (cf. [14] ainsi que [11], § 1) : d'après cette théorie, les corps K' tels que $K \supset K' \supset K^p$ correspondent bijectivement aux K-sous-espaces vectoriels N de $\Delta(K)$ qui sont stables pour le crochet et la puissance p-ème. (De façon plus précise, K' et N sont annulateurs l'un de l'autre pour l'application canonique de $K \times \Delta(K)$ dans K.) Le corps K' est donc invariant à droite et à gauche si et seulement si N l'est, c'est-à-dire (Lemme 4) si N est de la forme $\mathfrak{n} \otimes_k K$, où $\mathfrak{n}$ est une p-sous-algèbre de Lie de $\mathfrak{t}(G)$ stable pour la représentation adjointe. On obtient donc finalement:

THÉORÈME 3. *Les classes d'isogénies radicielles $G \to G'$ de hauteur 1 correspondent bijectivement aux p-sous-algèbres de Lie de $\mathfrak{t}(G)$ qui sont stables pour la représentation adjointe.*

De plus, le Lemme 5 montre que la sous-algèbre $\mathfrak{n}(\phi)$ qui correspond à une isogénie ϕ n'est autre que le noyau de l'application tangente à ϕ à l'origine.

Si $\mathfrak{n}$ est une p-sous-algèbre de Lie de $\mathfrak{t}(G)$ stable pour la représentation adjointe, nous désignerons par $G/\mathfrak{n}$ le groupe G' qui lui est associé; au point de vue ensembliste, on a $G' = G$, mais les fonctions rationnelles (resp. régulières) sur G' sont les fonctions rationnelles (resp. régulières) sur G qui sont annulées par les dérivations invariantes appartenant à $\mathfrak{n}$. D'après la théorie de Jacobson, le *degré* $\nu(\phi) = [K : K']$ de l'isogénie est égal à $p^{\dim \mathfrak{n}}$.

Si l'on prend $\mathfrak{n} = 0$, on trouve $G/\mathfrak{n} = G$; si l'on prend $\mathfrak{n} = \mathfrak{t}(G)$, on trouve $G/\mathfrak{n} = G^p$; ce sont les deux cas extrêmes. Il peut se faire que $\mathfrak{t}(G)$ n'admette pas d'autre p-sous-algèbre de Lie, stable pour la représentation adjointe; c'est par exemple le cas si $\mathfrak{t}(G)$ est une algèbre de Lie simple.

Si $\theta : G \to H$ est un homomorphisme, et si le noyau de l'application tangente à θ contient $\mathfrak{n}$, on peut factoriser θ en $G \to G/\mathfrak{n} \to H$: cela résulte du Lemme 5 et de la caractérisation des fonctions rationnelles sur $G/\mathfrak{n}$.

Remarques. 1) Soit $\mathfrak{n}$ une p-sous-algèbre de Lie de $\mathfrak{t}(G)$, non nécessairement stable pour la représentation adjointe; on peut encore définir $G/\mathfrak{n}$ et montrer que la loi de composition de G définit par passage au quotient une application régulière $G \times G/\mathfrak{n} \to G/\mathfrak{n}$, d'où une structure d'*espace homogène* sur $G/\mathfrak{n}$.

2) Comme on l'a dit dans l'introduction, le Théorème 3 est essentiellement dû à Barsotti ([3], § 2), à cela près qu'il se bornait au cas des groupes commutatifs (mais il considérait des isogénies radicielles de hauteur quel-

conque). Les résultats de Barsotti ont été généralisés par Cartier; voir sa note [6], dont il faut toutefois corriger légèrement les énoncés (sauf celui du Th. 3).

6. Application à la variété d'Albanese. Soit $f: V \to G$ une application rationnelle d'une variété irréductible V dans un groupe algébrique commutatif G, également irréductible.

THÉORÈME 4. *Les deux propriétés suivantes sont équivalentes:*

(i) *Il est impossible de factoriser f en $V \to G_1 \to G$, où $V \to G_1$ est une application rationnelle, et où $G_1 \to G$ est une isogénie radicielle de hauteur 1 non triviale (i.e. de degré $\neq 1$).*

(ii) *Pour toute forme différentielle ω de degré 1 sur G, invariante par translation, et non nulle, on a $f^*(\omega) \neq 0$.*

Soit $\Omega(G)$ l'espace vectoriel des formes différentielles de degré 1 sur G qui sont invariantes par translation; c'est le dual de l'algèbre de Lie $\mathfrak{t}(G)$. On observera que, puisque G est supposé commutatif, la représentation adjointe de G dans $\mathfrak{t}(G)$ est triviale, de même que le crochet; vu la dualité entre crochet et différentielle extérieure, on a $d\omega = 0$ pour tout $\omega \in \Omega(G)$. Ainsi, *l'opération de Cartier* C est définie pour tout $\omega \in \Omega(G)$, et l'on a $C(\omega) \in \Omega(G)$, cf. [5]; cette opération est transposée de l'opération de puissance p-ème dans $\mathfrak{t}(G)$, *loc. cit.*, formule (6).

Montrons maintenant que (ii) $\Rightarrow$ (i), et soit $V \to G_1 \to G$ une factorisation de f, où $\phi: G \to G$ est une isogénie radicielle de hauteur 1 avec $\nu(\phi) \neq 1$. L'application $\mathfrak{t}(\phi): \mathfrak{t}(G_1) \to \mathfrak{t}(G)$ a un noyau non nul, donc n'est pas surjective, et il existe une forme linéaire non nulle ω sur $\mathfrak{t}(G)$ qui s'annule sur l'image de $\mathfrak{t}(G_1)$; on a $\phi^*(\omega) = 0$, d'où *a fortiori* $f^*(\omega) = 0$ et cette contradiction montre bien que (ii) $\Rightarrow$ (i).

Inversement, supposons (i) vérifié, et soit $\mathfrak{n}^*$ le sous-espace de $\Omega(G)$ formé des différentielles ω telles que $f^*(\omega) = 0$. La formule $Cf^* = f^*C$ montre que $\mathfrak{n}^*$ est stable par l'opération de Cartier C, donc que l'orthogonal $\mathfrak{n}$ de $\mathfrak{n}^*$ dans $\mathfrak{t}(G)$ est stable par l'opération de puissance p-ème. Soit $G_2 = G/\mathfrak{n}$, et soit g l'application composée $V \to G \to G_2$; si $\omega' \in \Omega(G_2)$ l'image réciproque de ω' par $G \to G_2$ s'annule sur $\mathfrak{n}$, donc appartient à $\mathfrak{n}^*$, d'où $g^*(\omega') = 0$. Comme $\Omega(G_2)$ engendre en chaque point de G_2 l'espace des covecteurs tangents, on en conclut que l'application linéaire tangente à g est triviale en tout point de V où elle est définie, i.e. sur tout ouvert U de V formé de

points simples et sur lequel g est régulière. Soient alors $x \in U$, $y = g(x)$, et soit $\theta \in \mathcal{O}_y(G_2)$; du fait que $g^*(d\theta) = 0$, la fonction $\theta \circ g$ est une puissance p-ème dans $\mathcal{O}_x(V)$. Munissons alors G_2 du faisceau d'anneaux formé par les puissances p^{-1}-èmes des éléments de $\mathcal{O}(G_2)$; on obtient ainsi $(G_2)^{p^{-1}}$ (cf. n°. 5), et ce qui précède montre que $g: V \to G_2$ est en fait une application régulière de V dans $(G_2)^{p^{-1}}$. Mais l'isogénie $G_2 \to G^p$ donne naissance à une isogénie $(G_2)^{p^{-1}} \to G$, et l'on a ainsi obtenu une factorisation de f "à travers" $(G_2)^{p^{-1}}$. Vu (i), cette isogénie doit être triviale, i. e. on doit avoir $(G_2)^{p^{-1}} = G$, ou $G_2 = G^p$, c'est-à-dire $\mathfrak{n} = \mathfrak{t}(G)$ ou encore $\mathfrak{n}^* = 0$, et (ii) est bien vérifié, cqfd.

Exemple. Soit A la *variété d'Albanese* de V ; l'application canonique $f: V \to A$ vérifie évidemment (i), et le Théorème 4 redonne un résultat d'Igusa [12].[2]

Supposons en particulier que V soit *complète* et *normale*, et désignons par $H^0(V, \Omega^1)$ l'espace vectoriel des formes différentielles de degré 1 sur V qui n'ont pas de diviseur polaire ; l'application $\omega \to f^*(\omega)$ est un homomorphisme de $\Omega(A)$ dans $H^0(V, \Omega^1)$ et est injectif d'après ce que l'on vient de voir ; on obtient ainsi l'inégalité $h^{1,0} \geqq \dim. A$.

Remarques. 1) En fait, le Théorème 4 peut servir à démontrer *l'existence* de la variété d'Albanese de V. Indiquons rapidement comment :

Soit $g: V \to B$ une application rationnelle de V dans une variété abélienne B ; on peut chercher à factoriser g en $V \to A \to B$, où $A \to B$ est une isogénie. Si l'on suppose que V engendre B, on voit aisément qu'il existe une factorisation *maximale* $V \to A \to B$; l'application $V \to A$ vérifie alors (i), et le Th. 4 montre que $\dim. A \leqq h^{1,0}$. On obtient ainsi une majoration de $\dim. B = \dim. A$ qui remplace la majoration par le genre de la courbe générique ([16], Chap. II, § 3). L'existence de la variété d'Albanese en résulte immédiatement (*loc. cit.*).

2) On observera que la condition (ii) ne signifie nullement que f soit une application *séparable*, c'est-à-dire correspondant à une extension de corps qui soit séparable : on sait que c'est inexact même pour l'application canonique de V dans sa variété d'Albanese. En voici un exemple simple : partons d'une variété abélienne A, de dimension 2, de corps des fonctions K, et soient $x, y \in K$ deux fonctions qui soient des paramètres uniformisants à l'élément neutre de A. Soit K' le sous-corps de K engendré par K^p et par l'élément $z = xy$; soit V la normalisée de A^p dans l'extension K'/K^p. On a des applica-

[2] Cette démonstration ne vaut qu'en caractéristique $p \neq 0$. En caractéristique zéro le théorème d'Igusa résulte simplement de ce que $\phi(V)$ *engendre* A.

tions canoniques $A \to V \to A^p$, et $[K : K'] = [K' : K^p] = p$; il s'ensuit que la variété d'Albanese de V est ou bien V ou bien A^p; mais on voit facilement que V a un point singulier à l'origine, donc V ne peut pas être une variété abélienne, et sa variété d'Albanese est A^p, ce qui fournit l'exemple cherché.

§ 3. Représentations p-adiques.

7. Les groupes $\mathrm{Ext}(A, B)$. Dans ce n°. H, nous allons résumer un certain nombre de définitions et de résultats élémentaires sur les extensions de groupes algébriques (commutatifs). Pour plus de détails, le lecteur pourra se reporter à [19], § 2 (et aussi à [2], dont le point de vue est toutefois assez différent).

Soient A, B, C trois groupes algébriques commutatifs, non nécessairement connexes. Une suite exacte d'homomorphismes (rationnels, ou réguliers, c'est la même chose) :

$$0 \to B \to C \to A \to 0 \tag{1}$$

est dite *strictement exacte* si B s'identifie à un sous-groupe de C (muni de la structure algébrique induite), et si A s'identifie au groupe quotient C/B (muni de la structure algébrique quotient). Il revient au même de dire que $B \to C$ et $C \to A$ sont *séparables*, ou encore que la suite d'algèbres de Lie :

$$0 \to \mathfrak{t}(B) \to \mathfrak{t}(C) \to \mathfrak{t}(A) \to 0 \tag{2}$$

est une suite exacte (d'espaces vectoriels).

Une suite strictement exacte (1) est appelée une *extension* de A par B; la notion d'isomorphisme de deux extensions a un sens clair; l'ensemble des classes d'extensions de A par B est noté $\mathrm{Ext}(A, B)$. On munit $\mathrm{Ext}(A, B)$ d'une loi de composition par le procédé classique de Baer [1] : si C et C' sont deux extensions, on désigne par D le sous-groupe de $C \times C'$ image réciproque de la diagonale de $A \times A$, et par Q le sous-groupe de D formé des couples $(b, -b)$, $b \in B$; on constate alors que le quotient D/Q forme de façon naturelle une extension de A par B, qui est dite somme des deux extensions données. Les raisonnements de Baer s'appliquent presque sans changement, et montrent que $\mathrm{Ext}(A, B)$ est un *groupe abélien* (la seule difficulté supplémentaire est qu'il faut montrer que l'on a bien des suites *strictement* exactes, mais c'est chaque fois évident sur les applications tangentes).

Si $f : A' \to A$ est un homomorphisme, et si C est une extension de A par B, on définit $f^*(C) \in \mathrm{Ext}(A', B)$ comme le sous-groupe de $A' \times C$ formé des couples (a', c) tels que a' et c aient même image dans A. On vérifie

que $f^*: \mathrm{Ext}(A,B) \to \mathrm{Ext}(A',B)$ est un homomorphisme, et que l'on a les formules $1^* = 1$, $(fg)^* = g^* f^*$, $(f+f')^* = f^* + f'^*$; ainsi, $\mathrm{Ext}(A,B)$ est un *foncteur contravariant additif* en A.

De même, tout homomorphisme $s: B \to B'$ définit un homomorphisme $s_*: \mathrm{Ext}(A,B) \to \mathrm{Ext}(A,B')$, et l'on montre que $\mathrm{Ext}(A,B)$ est un *foncteur covariant additif* en B. Si $f: A' \to A$ est un homomorphisme, on a $f^* s_* = s_* f^*$, ce qui montre que $\mathrm{Ext}(A,B)$ est *biadditif*.

Si A et B sont deux groupes algébriques commutatifs, on note $\mathrm{Hom}(A,B)$ le groupe des homomorphismes (réguliers) de A dans B.

Soit maintenant $0 \to A' \to A \to A'' \to 0$ une suite strictement exacte, et soit $\phi \in \mathrm{Hom}(A',B)$; on a $\phi_*(A) \in \mathrm{Ext}(A'',B)$, et l'on obtient ainsi un homomorphisme $d: \mathrm{Hom}(A',B) \to \mathrm{Ext}(A'',B)$. Cet homomorphisme de "bord," combiné avec les homomorphismes fonctoriels associés à $A' \to A$ et $A \to A''$, fournit une *suite exacte*:

$$(3)\quad 0 \to \mathrm{Hom}(A'',B) \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(A',B) \xrightarrow{d} \mathrm{Ext}(A'',B) \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(A',B).$$

De même, on associe à toute suite strictement exacte $0 \to B' \to B \to B'' \to 0$ une *suite exacte*:

$$(4)\quad 0 \to \mathrm{Hom}(A,B') \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,B'') \xrightarrow{d} \mathrm{Ext}(A,B') \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(A,B'').$$

8. Comportement de $\mathrm{Ext}(A,B)$ par isogénie radicielle de hauteur 1. Soient A et B deux groupes algébriques commutatifs connexes, et soit $\mathfrak{n}$ une p-sous-algèbre de Lie de $\mathfrak{t}(A)$, c'est-à-dire un sous-espace vectoriel de $\mathfrak{t}(A)$ stable pour la puissance p-ème. On a défini au n°. 5 l'isogénie radicielle $A \to A/\mathfrak{n}$; à cette isogénie nous allons associer une *suite exacte* (analogue à la suite (3) du n°. 7):

$$(5)\quad 0 \to \mathrm{Hom}(A/\mathfrak{n},B) \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B)) \xrightarrow{d} \mathrm{Ext}(A/\mathfrak{n},B) \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B)).$$

Il faut d'abord préciser que $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ et $\mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B))$ sont pris au sens de la catégorie des *espaces vectoriels munis d'une opération de puissance p-ème* (i.e. des p-algèbres de Lie abéliennes); par exemple, un élément de $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ est une application linéaire de $\mathfrak{n}$ dans $\mathfrak{t}(B)$ qui commute avec la puissance p-ème. Tout homomorphisme de A dans B définit un

homomorphisme de $\mathfrak{t}(A)$ dans $\mathfrak{t}(B)$, d'où, par restriction, un homomorphisme de $\mathfrak{n}$ dans $\mathfrak{t}(B)$. Les homomorphismes $\mathrm{Hom}(A,B) \to \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ et $\mathrm{Ext}(A,B) \to \mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B))$ sont définis de façon évidente. Quant à l'homomorphisme "bord" d: $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B)) \to \mathrm{Ext}(A/\mathfrak{n},B)$ il est défini ainsi: soit $\phi \in \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$, et soit $\mathfrak{n}_\phi$ le sous-espace de $\mathfrak{t}(A) \times \mathfrak{t}(B) = \mathfrak{t}(A \times B)$ formé par les couples $(X, \phi(X))$, où X parcourt $\mathfrak{n}$. Il est clair que $\mathfrak{n}_\phi$ est une p-sous-algèbre de Lie de $\mathfrak{t}(A \times B)$, ce qui permet de définir $C_\phi = (A \times B)/\mathfrak{n}_\phi$; les homomorphismes canoniques $B \to A \times B$ et $A \times B \to A/\mathfrak{n}$ définissent des homomorphismes $B \to C_\phi$ et $C_\phi \to A/\mathfrak{n}$, et l'on vérifie immédiatement que la suite

$$0 \to B \to C_\phi \to A/\mathfrak{n} \to 0$$

est strictement exacte. On a ainsi obtenu l'application

$$d\colon \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B)) \to \mathrm{Ext}(A/\mathfrak{n},B)$$

cherchée; on vérifie que c'est un homomorphisme.

Il reste maintenant à démontrer l'exactitude de la suite (5); jusqu'à $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ elle est triviale. Pour $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$, on doit montrer que les conditions "C_ϕ est isomorphe à $A/\mathfrak{n} \times B$" et "ϕ est la restriction à $\mathfrak{n}$ d'un homomorphisme de A dans B" sont équivalentes. Tout d'abord, si ϕ se prolonge en $g\colon A \to B$, l'application $a \to (a, g(a))$ de A dans $A \times B$ applique $\mathfrak{n}$ dans $\mathfrak{n}_\phi$, donc définit par passage au quotient un homomorphisme $A/\mathfrak{n} \to C_\phi$ qui est une section; on a donc bien $C_\phi = A/\mathfrak{n} \times B$. Inversement, si l'extension C_ϕ est triviale, il y a une "rétraction" $r\colon C \to B$ qui est l'identité sur B, et, en composant r avec l'application naturelle de A dans C_ϕ, on trouve un homomorphisme $g\colon A \to B$ qui prolonge $-\phi$.

Soit $\phi \in \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$; par construction, il existe un homomorphisme $A \to C_\phi$ relevant la projection $A \to A/\mathfrak{n}$; donc C_ϕ appartient au noyau de $\mathrm{Ext}(A/\mathfrak{n},B) \to \mathrm{Ext}(A,B)$. Inversement, si C est un élément de ce noyau, il existe un homomorphisme $k\colon A \to C$ relevant $A \to A/\mathfrak{n}$; la restriction de $-k$ à $\mathfrak{n}$ est un homomorphisme ϕ de $\mathfrak{n}$ dans $\mathfrak{t}(G)$; soit C_ϕ l'extension de $A/\mathfrak{n}$ par B associée à ϕ. L'application $(a,b) \to k(a) + b$ est un homomorphisme de $A \times B$ dans C dont la restriction à $\mathfrak{n}_\phi$ est nulle; par passage au quotient, elle définit un homomorphisme $s\colon C_\phi \to C$ qui est l'identité sur B et définit par passage au quotient l'identité sur $A/\mathfrak{n}$; les deux extensions C et C_ϕ sont donc isomorphes, ce qui démontre l'exactitude de (5) en $\mathrm{Ext}(A/\mathfrak{n},B)$.

Soit $C \in \mathrm{Ext}(A/\mathfrak{n},B)$, et soit $E \in \mathrm{Ext}(A,B)$ l'image réciproque de C par $A \to A/\mathfrak{n}$; par définition, E est le noyau de l'homomorphisme $A \times C \to A/\mathfrak{n}$ différence des homomorphismes $A \to A/\mathfrak{n}$ et $C \to A/\mathfrak{n}$. L'application

$\mathfrak{t}(A \times C) \to \mathfrak{t}(A/\mathfrak{n})$ étant surjective, la suite $0 \to E \to A \times C \to A/\mathfrak{n} \to 0$ est strictement exacte, et $\mathfrak{t}(E)$ s'identifie au noyau de $\mathfrak{t}(A) \times \mathfrak{t}(C) \to \mathfrak{t}(A/\mathfrak{n})$; il s'ensuit que $\mathfrak{t}(E)$ contient $\mathfrak{n} \times \{0\}$, et que l'élément de $\mathrm{Ext}(\mathfrak{n}, \mathfrak{t}(B))$ défini par E est trivial. Inversement, soit E une extension de A par B jouissant de cette propriété, et soit $\theta: \mathfrak{n} \to \mathfrak{t}(E)$ une "section" (compatible avec la puisance p-ème) ; si l'on pose $C = E/\theta(\mathfrak{n})$, on vérifie tout de suite que $C \in \mathrm{Ext}(A/\mathfrak{n}, B)$ et que l'image de C dans $\mathrm{Ext}(A, B)$ n'est autre que E, ce qui achève de démontrer l'exactitude de la suite (5).

9. Comparaison de $\mathrm{Ext}(A, B)$ avec la cohomologie de A. Nous allons maintenant reprendre, en les complétant sur quelques points, les résultats de [19], § 3. Dans tout ce qui suit, A désigne une *variété abélienne*, et B un groupe linéaire commutatif et connexe. Les deux cas que nous avons principalement en vue sont les suivants :

a) $B = G_m$, groupe *multiplicatif*.

b) $B = W_n$, groupe additif des *vecteurs de Witt* de longueur n (pour $n = 1$, c'est le groupe *additif* G_a).

Soit $\mathscr{B}$ le faisceau des germes d'applications régulières de A dans B ; le groupe $H^1(A, \mathscr{B})$ n'est autre que le groupe des classes d'espaces fibrés principaux (localement triviaux) de base A et de groupe structural B. Toute extension C de A par B définit un tel espace fibré : on sait en effet ([2], Lemme 3.2 ainsi que [17], Th. 10) qu'il existe une section rationnelle $A \to C$, d'où par translation l'existence d'une section régulière en un point donné de A, ce qui montre bien que C est localement trivial. On obtient ainsi une application canonique $\theta: \mathrm{Ext}(A, B) \to H^1(A, \mathscr{B})$ dont on vérifie tout de suite que c'est un homomorphisme.

Lemme 7. *L'application θ est injective.*

Soit C une extension de A par B qui soit triviale en tant qu'espace fibré, c'est-à-dire qui possède une section régulière $s: A \to C$. Quitte à effectuer une translation, on peut supposer que $s(0) = 0$. Soit A' le sous-groupe de C engendré par $s(A)$; comme A est complète et s régulière, $s(A)$ est complète et il en est de même de A', donc aussi de $A \cap B$; comme B est une variété affine, on a donc $\dim.(A' \cap B) = 0$, d'où $\dim. A' = \dim. A = \dim. s(A)$ et $A' = s(A)$. Ainsi s est un homomorphisme, cqfd.

Remarque. Le raisonnement précédent (dû à Rosenlicht, [19], Prop. 9) démontre en fait ceci : soit V une variété complète et non singulière, et soit

$\phi: V \to A$ l'application canonique de V dans sa variété d'Albanese. L'application composée $\mathrm{Ext}(A,B) \to H^1(A,\mathfrak{B}) \to H^1(V,\mathfrak{B})$ est alors *injective* (le second homomorphisme étant ϕ^*). C'est là un résultat analogue à celui d'Igusa (cf. n°. 6), et qui fournit l'inégalité $\dim. A \leqq h^{0,1}$ (et même $\dim. A \leqq \dim. Z_x^1$, avec les notations de [22], n°. 7).

Soient maintenant p_1 et p_2 les deux projections de $A \times A$ sur A, et soit $s = p_1 + p_2$.

LEMME 8. *Pour qu'un élément $x \in H^1(A,\mathfrak{B})$ appartienne à l'image de θ, il faut et il suffit qu'il soit "primitif," c'est-à-dire qu'il vérifie la relation:*

$$s^*(x) = p_1^*(x) + p_2^*(x) \text{ dans } H^1(A \times A, \mathfrak{B}).$$

La nécessité résulte de ce que $\mathrm{Ext}(A,B)$ est un foncteur *additif* de A. Supposons inversement que E soit un espace fibré principal, de base A et de groupe structural B, correspondant à un élément primitif de $H^1(A,\mathfrak{B})$. Cette dernière hypothèse revient à dire qu'il existe une application régulière $g: E \times E \to E$, vérifiant la formule

$$g(e+b, e'+b') = g(e,e') + b + b',$$

et définissant par passage au quotient l'application $s: A \times A \to A$. Quitte à effectuer une translation, on peut en outre supposer que, pour un point $0 \in E$ se projetant au point 0 de A, on a $g(0,0) = 0$. Tout revient alors à montrer que la loi de composition g fait de E un groupe commutatif qui est une extension de A par B. Vérifions par exemple la commutativité de g: si $e, e' \in E$, $g(e,e')$ et $g(e',e)$ ont même image dans A, et l'on peut écrire: $g(e,e') = g(e',e) + k(e,e')$, où k est une application de $E \times E$ dans B; on voit facilement que k est régulière, et que $k(e+b, e'+b') = k(e,e')$, $b, b' \in B$; donc k définit par passage au quotient une application régulière $A \times A \to B$ qui ne peut être que constante, puisque $A \times A$ est complète et B affine; comme de plus $k(0,0) = 0$, on voit donc que $k(e,e') = 0$ pour tout couple (e,e'), ce qui démontre bien la commutativité de g. Les autres vérifications se font de manière analogue.

Les deux lemmes précédents nous permettent d'identifier $\mathrm{Ext}(A,B)$ au sous-groupe de $H^1(A,\mathfrak{B})$ formé des *éléments primitifs*. Nous allons maintenant déterminer ce sous-groupe dans les deux cas particuliers indiqués plus haut:

Cas a). On a $B = G_m$, et le groupe $H^1(A,\mathfrak{B})$ n'est autre que le groupe $D(A)$ des *classes de diviseurs* de la variété A, pour l'équivalence linéaire. Dire que la classe d'un diviseur X est un élément primitif de $D(A)$ signifie

que l'on a $s^{-1}(X) \sim p_1^{-1}(X) + p_2^{-1}(X) = X \times A + A \times X$ sur $A \times A$, autrement dit que $X \equiv 0$ au sens de Weil [23], p. 107 (cf. aussi [16], Chap. IV). Nous désignerons par $P(A)$ le sous-groupe de $D(A)$ formé par les classses de tels diviseurs; d'après les Lemmes 7 et 8, on a $P(A) = \mathrm{Ext}(A, G_m)$, résultat dû à Weil [24].

On sait (cf. par exemple [16]) que $P(A)$ contient le sous-groupe A^* de $D(A)$ formé des classes de diviseurs *algébriquement équivalents à zéro*, le quotient $P(A)/A^*$ étant le *groupe de torsion* de A. En fait, Barsotti [3] a démontre que ce groupe est toujours nul, i.e. que $P(A) = A^*$; nous donnerons au n°. 10 une autre démonstration de ce fait.

Cas b). On a $B = W_n$, et le faisceau $\mathcal{B}$ n'est autre *que* le faisceau $\mathcal{B}\mathcal{W}_n$ considéré au n°. 3. *Tout élément de* $H^1(A, \mathcal{W}_n)$ *est primitif.* En effet, il suffit de montrer que $H^1(A \times A, \mathcal{W}_n)$ est égal à $H^1(A, \mathcal{W}_n) \times H^1(A, \mathcal{W}_n)$; pour $n = 1$, cela résulte de la formule de Künneth (n°. 1), et on va raisonner par récurrence sur n, en utilisant la suite exacte $0 \to \mathcal{W}_{n-1} \to \mathcal{W}_n \to \mathcal{O} \to 0$. Les deux injections canoniques de A dans $A \times A$ définissent un homomorphisme

$$i^* : H^1(A \times A, \mathcal{W}_n) \to H^1(A, \mathcal{W}_n) \times H^1(A, \mathcal{W}_n) ;$$

les deux projections canoniques de $A \times A$ sur A définissent un homomorphisme

$$p^* : H^1(A, \mathcal{W}_n) \times H^1(A, \mathcal{W}_n) \to H^1(A \times A, \mathcal{W}_n).$$

On a $i^* \circ p^* = 1$, et tout revient à montrer que i^* est injectif. Or on a un diagramme commutatif:

$$\begin{array}{ccccccc} 0 & \to & H^1(A \times A, \mathcal{W}_{n-1}) & \to & H^1(A \times A, \mathcal{W}_n) & \to & H^1(A \times A, \mathcal{O}) \\ & & \downarrow i^* & & \downarrow i^* & & \downarrow i^* \\ 0 & \to & H^1(A, \mathcal{W}_{n-1}) \times H^1(A, \mathcal{W}_{n-1}) & \to & H^1(A, \mathcal{W}_n) \times H^1(A, \mathcal{W}_n) & \to & H^1(A, \mathcal{O}) \times H^1(A, \mathcal{O}) \end{array}$$

Vu l'hypothèse de récurrence les deux flèches verticales extrêmes sont bijectives; la flèche verticale médiane est donc injective, ce qui achève la démonstration.

On obtient finalement $\mathrm{Ext}(A, W_n) = H^1(A, \mathcal{W}_n)$, cf. [19], Th. 1.

10. Effet d'une isogénie sur la cohomologie. Non-existence de torsion. Nous nous proposons de déterminer l'effet d'une isogénie $\phi : A \to A'$ (A et A' étant des variétés abéliennes) sur les groupes $H^1(A, \mathcal{W}_n) = \mathrm{Ext}(A, W_n)$ et $P(A) = \mathrm{Ext}(A, G_m)$. Il est commode d'introduire quatre type "élémentaires" d'isogénies:

type s_1 (resp. s_2) : isogénie séparable $A \to A/N$, où N est un sous-groupe fini de A d'ordre premier à p (resp. d'ordre p).

type i_1 (resp. i_2) : isogénie radicielle $A \to A/\mathfrak{n}$, de hauteur 1, où $\mathfrak{n}$ est un sous-espace vectoriel de $\mathfrak{t}(A)$ ayant une base formée d'un élément X tel que $X^p = 0$ (resp. tel que $X^p = X$).

LEMME 9. *Toute isogénie est un produit d'isogénies appartenant à l'un des types précédents.*

Soit $\phi : A \to A'$ une isogénie quelconque, et soit $\nu(\phi)$ son degré; raisonnons par récurrence sur $\nu(\phi)$, le cas $\nu(\phi) = 1$ étant trivial. Si ϕ est séparable, on a $A' = A/Q$, où Q est un sous-groupe fini de A; si l'ordre de Q est premier à p, ϕ est du type s_1; sinon Q contient un sous-groupe N d'ordre p, et on peut factoriser ϕ en $A \to A/N \to A/Q$; comme le degré de l'isogénie $A/N \to A/Q$ est égal à $\nu(\phi)/p$, on peut lui appliquer l'hypothèse de récurrence. Supposons maintenant que ϕ soit inséparable, et soit $\mathfrak{q}$ le noyau de $\mathfrak{t}(A) \to \mathfrak{t}(A')$; on sait (Lemme 5) que $\mathfrak{q}$ est stable pour la puissance p-ème, et l'on a $\mathfrak{q} \neq 0$ (sinon ϕ serait séparable). La structure des p-algèbres de Lie abéliennes (c'est-à-dire la " réduction de Jordan " des applications p-linéaires) montre alors que $\mathfrak{q}$ contient un sous-espace $\mathfrak{n}$ ayant une base formée d'un élément X tel que $X^p = X$ ou $X^p = 0$ (cf. par exemple [7], nos. 10, 11). On peut alors factoriser ϕ en $A \to A/\mathfrak{n} \to A'$, et appliquer l'hypothèse de récurrence à $A/\mathfrak{n} \to A'$, cqfd.

En particulier, toute isogénie de degré p est de l'un des types s_2, i_1, ou i_2.

Si $\phi : A \to A'$ est une isogénie, nous noterons ϕ_n^* l'application de $H^1(A', \mathfrak{W}_n)$ dans $H^1(A, \mathfrak{W}_n)$ définie par ϕ; c'est un Λ-homomorphisme, Λ désignant l'anneau $W(k)$, cf. no. 3.

LEMME 10. *Si ϕ est de type s_1 ou de type i_2, ϕ_n^* est bijectif. Si ϕ est de type s_2 ou de type i_1, ϕ_n^* a pour noyau et pour conoyau des Λ-modules de longueur* 1.

D'après les Théorèmes 1 et 2, $H^1(A, \mathfrak{W}_n)$ est un Λ-module de longueur $n\dim.(A)$, et de même pour $H^1(A', \mathfrak{W}_n)$. Comme ϕ_n^* est un Λ-homomorphisme, son noyau et son conoyau ont même longueur, et il suffira de considérer le noyau.

Supposons d'abord ϕ séparable, donc de la forme $A \to A/N$. Tenant compte de ce que $H^1(A, \mathfrak{W}_n) = \mathrm{Ext}(A, W_n)$, on peut appliquer la suite exacte des Ext (cf. no. 7, suite (3)), et l'on obtient la suite exacte :[3]

$$0 \to \mathrm{Hom}(N, W_n) \to H^1(A/N, \mathfrak{W}_n) \to H^1(A, \mathfrak{W}_n). \tag{6}$$

[3] Cette suite exacte peut aussi se déduire de la *suite spectrale* de Cartan-Leray du revêtement galoisien $A \to A/N$.

On est alors ramené à vérifier que $\mathrm{Hom}(N, W_n)$ est un Λ-module de longueur 0 (resp. 1) dans le cas s_1 (resp. s_2), ce qui est évident.

Supposons ensuite ϕ inséparable, donc de la forme $A \to A/\mathfrak{n}$, avec $\mathfrak{n}$ de dimension 1. On peut alors appliquer la suite exacte (5) du n°. 8, et l'on obtient la suite exacte:[4]

$$(7) \qquad 0 \to \mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(W_n)) \to H^1(A/\mathfrak{n}, \mathcal{W}_n) \to H^1(A, \mathcal{W}_n).$$

La structure de la p-algèbre de Lie $\mathfrak{t}(W_n)$ est bien connue (cf. par exemple [7], n°. 16) : elle a une base formée de n éléments $X_1, \cdots, X_n$, avec $X_1^p = X_2$, $X_2^p = X_3, \cdots, X_n^p = 0$. On en déduit bien que $\mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(W_n))$ est de dimension 0 ou 1 (sur k) suivant que ϕ est de type i_2 ou de type i_1, cqfd.

Si $\phi: A \to A'$ est une isogénie, nous noterons ${}^t\phi$ l'homomorphisme de $P(A')$ dans $P(A)$ défini par ϕ (cette notation est en accord avec celle utilisée dans la théorie de la variété de Picard, cf. [16], Chap. V, § 1).

LEMME 11. *Si ϕ est de type s_2 ou de type i_1, le noyau de ${}^t\phi$ est nul; si ϕ est de type i_2, ce noyau est d'ordre p; si ϕ est de type s_1, il est fini et d'ordre premier à p. Dans tous les cas, ${}^t\phi$ est surjectif.*

On raisonne comme dans le Lemme 10, en utilisant l'isomorphisme $P(A) = \mathrm{Ext}(A, G_m)$ et les suites exactes (3) et (5). On obtient ainsi, dans le cas séparable, la suite exacte:

$$(8) \qquad 0 \to \mathrm{Hom}(N, G_m) \to P(A/N) \to P(A) \to \mathrm{Ext}(N, G_m).$$

Comme G_m est un groupe *divisible*, $\mathrm{Ext}(N, G_m)$ est nul, et ${}^t\phi$ est surjectif; quant au noyau de ${}^t\phi$, il est isomorphe à $\mathrm{Hom}(N, G_m)$, c'est-à-dire à la composante d'ordre premier à p du groupe des caractères de N; d'où le lemme dans le cas séparable.

Dans le cas inséparable, on a de même une suite exacte:

$$(9) \qquad 0 \to \mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(G_m)) \to P(A/\mathfrak{n}) \to P(A) \to \mathrm{Ext}(\mathfrak{n}, \mathfrak{t}(G_m)).$$

La p-algèbre de Lie $\mathfrak{t}(G_m)$ a comme base l'élément $Y = t\partial/\partial t$, et l'on a $Y^p = Y$; on en déduit que $\mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(G_m))$ est nul (resp. cyclique d'ordre p) si l'on est dans le cas i_1 (resp. i_2), et que, dans tous les cas, $\mathrm{Ext}(\mathfrak{n}, \mathfrak{t}(G_m)) = 0$, cqfd.

THÉORÈME 5. *Une variété abélienne n'a pas de torsion.*

[4] De même que ci-dessus, cette suite exacte peut se déduire d'une *suite spectrale* analogue à celle de Cartan-Leray, où la cohomologie de la p-algèbre de Lie $\mathfrak{n}$ (au sens de Hochschild [10]) remplace la cohomologie des groupes.

(Autrement dit, on a $P(A) = A^*$, ou encore, si X est un diviseur, les relations "$X \equiv 0$" et "X est algébriquement équivalent à zéro" sont équivalentes).

Le groupe A^* des classes de diviseurs algébriquement équivalents à 0 est un sous-groupe de $P(A)$, et l'on sait (cf. [16], Chap. IV, par exemple) qu'il existe un entier $n \geqq 1$ tel que $n \cdot P(A) \subset A^*$. Soit $\phi: A \to A$ l'isogénie définie par la multiplication par n; en combinant les Lemmes 9 et 11 on voit que ${}^t\phi: P(A) \to P(A)$ est surjectif. Mais $P(A) = \mathrm{Ext}(A, G_m)$ et les foncteurs $\mathrm{Ext}(A, B)$ sont additifs; il s'ensuit que ${}^t\phi$ n'est autre que la multiplication par n (voir aussi [23], Prop. 31), d'où $P(A) = n \cdot P(A) \subset A^*$, cqfd.

Remarque. Comme on l'a indiqué dans l'introduction, le **Théorème 5** est dû à Barsotti [3]; la démonstration de Barsotti, assez différente de celle donnée ci-dessus,[5] est basée sur une caractérisation des différentielles "logarithmiques" (voir aussi [5]).

11. Représentations *p*-adiques. Soit A une variété abélienne; on sait ([22], Prop. 4) que $H^1(A, \mathcal{W}) = \lim H^1(A, \mathcal{W}_n)$ est un Λ-module libre de type fini; soit $r(A)$ son rang. Tout homomorphisme $\phi: A \to B$ définit un homomorphisme transposé $\phi^*: H^1(B, \mathcal{W}) \to H^1(A, \mathcal{W})$, limite des ϕ_n^* considérés au n°. précédent. On notera que ϕ^* *commute* aux opérations V et F.

Soit d'autre part $A^* = P(A)$ le groupe des classes de diviseurs sur A algébriquement équivalents à zéro (la "variété de Picard" de A); nous noterons $T_p(A^*)$ le "groupe de Tate" de A^* relatif au nombre premier p. Rappelons ([16], Chap. VII, § 1) que l'on a $T_p(A^*) = \mathrm{Hom}(\boldsymbol{Q}_p/\boldsymbol{Z}_p, A^*)$; un élément de $T_p(A^*)$ n'est donc pas autre chose qu'une suite $(x_1, \cdots, x_n, \cdots)$, avec $x_i \in A^*$, $px_1 = 0$, $px_2 = x_1$, $px_3 = x_2, \cdots$ etc. Si $p^{s(A)}$ est le nombre de points d'ordre p de A^* (ou de A, c'est la même chose, puisque A et A^* sont isogènes), $T_p(A^*)$ est un module libre de rang $s(A)$ sur l'anneau $\boldsymbol{Z}_p$ des entiers p-adiques (*loc. cit.*). Tout homomorphisme $\phi: A \to B$ définit un homomorphisme transposé ${}^t\phi: T_p(B^*) \to T_p(A^*)$.

On sait que l'anneau $\boldsymbol{Z}_p$ peut être identifié à l'anneau $W(\boldsymbol{F}_p)$ des vecteurs de Witt de longueur infinie sur le corps $\boldsymbol{F}_p$ à p éléments, donc à un sous-anneau de $\Lambda = W(k)$: l'ensemble des éléments de Λ invariants par F. Par extension de l'anneau d'opérateurs, le $\boldsymbol{Z}_p$-module $T_p(A^*)$ définit un Λ-module $T'_p(A^*)$ de même rang $s(A)$.

Enfin, nous désignerons par $L_p(A)$ la somme directe de $H^1(A, \mathcal{W})$ et de $T'_p(A^*)$; c'est un Λ-module libre de rang $r(A) + s(A)$, et, comme chacun

[5] Cette démonstration a également été obtenue par Cartier (non publié).

de ses facteurs, c'est un foncteur contravariant additif en A. Si $\phi: A \to B$ est un homomorphisme, nous noterons ϕ' l'homomorphisme de $L_p(B)$ dans $L_p(A)$ qui lui est associé.

THÉORÈME 6. *Soit $\phi: A \to B$ une isogénie de degré $\nu(\phi)$, et soit p^k la plus haute puissance de p divisant $\nu(\phi)$. L'application $\phi': L_p(B) \to L_p(A)$ est alors injective, et son conoyau est un Λ-module de longueur finie égale à k.*

Vu le Lemme 9, il suffit de démontrer le théorème dans le cas d'une isogénie "élémentaire." Examinons successivement les quatre cas:

type s_1. Les Lemmes 10 et 11 montrent que $\phi^*: H^1(B, \mathfrak{M}) \to H^1(A, \mathfrak{M})$ ainsi que ${}^t\phi: T_p(B^*) \to T_p(A^*)$ sont bijectifs, et il en est donc de même de ϕ'; comme $k = 0$ dans ce cas, le théorème est bien vérifié.

type s_2. D'après le Lemme 10, pour tout $n \geqq 1$, le noyau et le conoyau de ${\phi_n}^*$ sont de longueur 1; par passage à la limite projective, on en déduit que le noyau de ϕ^* est de longueur 0 on 1 (donc 0 puisque $L_p(B)$ est un module libre), et que le conoyau de ϕ^* est de longueur 1 (les conoyaux s'appliquant les uns sur les autres quand $n \to +\infty$). D'autre part, le Lemme 11 montre que ${}^t\phi$ est bijectif, d'où le théorème, puisqu'ici $k = 1$.

type i_1. Même raisonnement que pour le type s_2.

type i_2. Le Lemme 10 montre que ϕ^* est bijectif. D'autre part le Lemme 11 montre que le noyau de ${}^t\phi: B^* \to A^*$ est cyclique d'ordre p; on en déduit par le raisonnement usuel ([23], p. 50 ou [16], *loc. cit.*) que ${}^t\phi: T_p(B^*) \to T_p(A^*)$ est injectif et que son conoyau est de longueur 1, d'où le théorème, puisqu'ici encore on a $k = 1$.

COROLLAIRE 1. *Le rang $r(A) + s(A)$ du Λ-module $L_p(A)$ est égal à $2 \cdot \dim(A)$.*

On applique le Théorème 6 à l'isogénie $\phi: A \to A$ définie par la multiplication par p. On a $\nu(\phi) = p^{2 \cdot \dim(A)}$ ([23], p. 127), et d'autre part le conoyau de ϕ' est $L_p(A)/p \cdot L_p(A)$, qui est un Λ-module de longueur $r(A) + s(A)$.

COROLLAIRE 2. *Soient A et B deux variétés abéliennes de même dimension, et soit ϕ un homomorphisme de A dans B. Si ϕ n'est pas une isogénie, le conoyau de ϕ' n'est pas de longueur finie.*

Soit C l'image de A dans B. On a $\dim. C < \dim. A = \dim. B$. L'application ϕ' se factorise en $L_p(B) \to L_p(C) \to L_p(A)$. D'après le Cor. 1, le rang

du Λ-module $L_p(C)$ est strictement inférieur à celui de $L_p(A)$, et le conoyau de ϕ' n'est donc pas de longueur finie.

(On pourrait facilement démontrer que $L_p(B) \to L_p(C)$ est surjectif, mais nous n'aurons pas besoin de ce résultat).

Nous allons maintenant prendre $B = A$, autrement dit considérer des éléments ϕ de l'anneau $\mathcal{A}(A)$ des *endomorphismes* de A. A un tel élément ϕ est attaché l'endomorphisme ϕ' de $L_p(A)$; on a les formules

$$(\phi_1 + \phi_2)' = \phi_1' + \phi_2' \text{ et } (\phi_1\phi_2)' = \phi_2'\phi_1';$$

ces formules signifient que $\phi \to \phi'$ est une *anti-représentation* de $\mathcal{A}(A)$ dans $L_p(A)$. Si l'on choisit une base dans $L_p(A)$, on obtient ainsi une représentation de $\mathcal{A}(A)$ par des matrices de degré $2.\dim(A)$ à coefficients dans Λ ; nous allons voir que cette représentation est l'analogue p-adique des représentations l-adiques de Weil :

THÉORÈME 7. *Si ϕ est un élément de $\mathcal{A}(A)$, le polynôme caractéristique de ϕ (au sens de Weil,* [23], p. 131) *est égal à celui de l'endomorphisme ϕ' de $L_p(A)$ qui lui est associé. On a en particulier*

$$\nu(\phi) = \det(\phi') \text{ et } \sigma(\phi) = \mathrm{Tr}(\phi').$$

Soit $D(\phi) = \det(\phi')$; c'est *a priori* un élément de Λ, et nous allons d'abord montrer que c'est un élément de $\mathbf{Z}_p$. Vu la décomposition de $L_p(A)$ en somme directe, on a $D(\phi) = \det(\phi^*) \cdot \det({}^t\phi)$, et il est clair que $\det({}^t\phi)$ appartient à $\mathbf{Z}_p$; reste à voir qu'il en est de même de $\det(\phi^*)$. Soit e_i, $i = 1, \cdots, r(A)$, une base de $H^1(A, \mathcal{W})$; si $\phi^*(e_i) = \sum a_{ij}e_j$, avec $a_{ij} \in \Lambda$, on a, par définition, $\det(\phi^*) = \det(a_{ij})$. Puisque $VF = p$, l'application F de $H^1(A, \mathcal{W})$ dans lui-même est une injection, et les Fe_i sont linéairement indépendants sur Λ. Du fait que ϕ^* commute avec F, on a $\phi^*(Fe_i) = \sum F(a_{ij}) \cdot Fe_i$, et l'on a $\det(\phi^*) = \det(F(a_{ij})) = F(\det(a_{ij})) = F(\det(\phi^*))$, ce qui signifie bien que $\det(\phi^*)$ est un élément de $\mathbf{Z}_p$, et démontre notre assertion.

A partir de là, la démonstration est la même que celle du Th. 36, p. 136, de [23] : le Th. 6 et son Cor. 2 montrent que les relations $\nu(\phi) = 0$ et $D(\phi) = 0$ sont équivalentes et que $D(\phi)$ et $\nu(\phi)$, lorsqu'ils sont non nuls, ont même valuation p-adique ; en appliquant le Lemme 12, p. 134, de [23], on en déduit que $D(\phi) = \nu(\phi)$, d'où le théorème.

Remarques.

1). A la différence des représentations l-adiques ($l \neq p$), la représentation p-adique que nous venons d'obtenir est à coefficients dans $\Lambda = W(k)$, et non dans $\mathbf{Z}_p$; l'exemple des courbes elliptiques d'invariant de Hasse nul montre d'ailleurs qu'il est impossible d'obtenir une représentation à coefficients dans $\mathbf{Z}_p$ ayant la trace voulue.

2). Nous avons construit la représentation précédente comme somme directe de deux représentations. En fait on peut la décomposer de façon canonique en somme directe de *trois facteurs*: chacun des $H^1(A, W_n)$ est somme directe d'un sous-espace $H^1(A, \mathcal{W}_n)_s$ où F est bijectif, et d'un sous-espace $H^1(A, \mathcal{W}_n)_n$ où F est nilpotent (**décomposition "de Fitting"**). Par passage à la limite, on obtient une décomposition $H^1(A, \mathcal{W})_s + H^1(A, \mathcal{W})_n$ de $H^1(A, \mathcal{W})$ qui est évidemment "fonctorielle"; le Λ-module $H^1(A, \mathcal{W})_s$ est isomorphe à $\mathrm{Hom}(T_p(A), \Lambda)$, comme on peut le voir en utilisant les résultats de [22], § 3. Cette décomposition de $L_p(A)$ en trois facteurs, outre qu'elle fait jouer un rôle plus symétrique à A et A^*, a l'avantage de "séparer" les isogénies des types s_2 et i_1: celles du premier type sont bijectives sur le facteur $H^1(A, \mathcal{W})_n$, celles du second type sur le facteur $H^1(A, \mathcal{W})_s$.

Collège de France,
Paris.

BIBLIOGRAPHIE.

[1] R. Baer, "Erweiterungen von Gruppen und ihren Isomorphismen," *Mathematische Zeitschrift*, vol. 38 (1934), pp. 375-416.

[2] I. Barsotti, "Structure theorems for group varieties," *Annali di Matematica*, vol. 38 (1955), pp. 77-119.

[3] ———, "Abelian varieties over fields of positive characteristic," *Rendiconti del Circolo Matematico di Palermo*, vol. 5 (1956), pp. 1-25.

[4] A. Borel, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[5] P. Cartier, "Une nouvelle opération sur les formes différentielles," *Comptes Rendus*, vol. 244 (1957), pp. 426-428.

[6] ———, "Calcul différentiel sur les variétés algébriques en caractéristique non nulle," *ibid.*, vol. 245 (1957), pp. 1109-1111.

[7] J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, II," *American Journal of Mathematics*, vol. 77 (1955), pp. 218-244.

[8] R. Godement, *Topologie algébrique et théorie des faisceaux*, Paris, Hermann, 1958.
[9] H. Hasse, "Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p," *Journal Crelle*, vol. 172 (1934), pp. 77-85.
[10] G. Hochschild, "Cohomology of restricted Lie algebras," *American Journal of Mathematics*, vol. 76 (1954), pp. 555-580.
[11] ———, "Simple algebras with purely inseparable splitting fields of exponent 1," *Transactions of the American Mathematical Society*, vol. 79 (1955), pp. 477-489.
[12] J. Igusa, "A fundamental inequality in the theory of Picard varieties," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 41 (1955), pp. 317-320.
[13] N. Jacobson, "Abstract derivation and Lie algebras," *Transactions of the American Mathematical Society*, vol. 42 (1937), pp. 206-224.
[14] ———, "Galois theory of purely inseparable fields of exponent 1," *American Journal of Mathematics*, vol. 66 (1944), pp. 645-648.
[15] S. Lang, *Introduction to algebraic geometry*, Interscience Tracts n° 5, New York, 1958.
[16] ———, *Abelian varieties*, Interscience Tracts, New York, 1958.
[17] M. Rosenlicht, "Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp .401-443.
[18] ———, "A note on derivations and differentials on algebraic varieties," *Portugaliae Mathematica*, vol. 16 (1957), pp. 43-55.
[19] ———, "Extensions of vector groups by abelian varieties," *American Journal of Mathematics*, vol. 80 (1958), pp. 685-713.
[20] J-P. Serre, "Faisceaux algébriques cohérents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.
[21] ———, "Sur la cohomologie des variétés algébriques," *Journal de Mathématiques*, vol. 36 (1957), pp. 1-16.
[22] ———, "Sur la topologie des variétés algébriques en caractéristique p," *Symposium de topologie algébrique*, Mexico, 1956.
[23] A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, Hermann, 1948.
[24] ———, "Variétés abéliennes," *Colloque d'algèbre et théorie des nombres*, Paris, 1949, pp. 125-128.

LIE GROUPS AND LIE HYPERALGEBRAS OVER A FIELD OF CHARACTERISTIC $p > 0$ (VIII).*†

By JEAN DIEUDONNÉ.

To E. Artin on his sixtieth birthday.

1. Introduction. In the last two papers of this series,[1] we obtained some precise information on what one may call the "building blocks" in the theory of formal Lie groups (over an algebraically closed field), namely the *simple* ones: thanks to the fundamental work of Chevalley [3], the simple noncommutative Lie groups are now known up to isomorphism, and the simple abelian groups have been determined in [10] up to isogeny. The main task ahead is now to see how these blocks are assembled in the most general groups, in other words, to study the problem of *extensions* of formal Lie groups. This paper is a small beginning in that direction: we have concentrated our efforts on the question of the position of the simple "divisible" abelian subgroups (i.e. the simple groups other than the additive group I_∞) in an arbitrary group; it is known that (with the exception of the tori) they lie in the center of the group, and the natural conjecture is that those which are in the center are quasi-direct factors of the whole group. I am able in this paper to prove that conjecture for *solvable* groups; the general theorem (if true) is linked with what seems to me the biggest open question remaining in the theory, the generalization of Levi's theorem.

Group extensions nowadays means cohomology, and we have followed the obvious method of attack, which consists in developing and using in our case

* Received March 4, 1958.

† Work done under contract AF 49(638)-106 with the U. S. Air Force.

[1] I use the terminology and results of these papers ([4] to [10]), and take this opportunity of correcting a few inaccuracies in [9] and [10]. In [9], p. 348, line 6, there should be a bar on the first u. On p. 352, the proof of (v) is not explicit enough: it should be observed that $[\mathfrak{g}_{r+1} \cap \mathfrak{H}, \mathfrak{t}_r]$ is contained in $\mathfrak{t}_r$, for we have $[\mathfrak{g}_{r+1} \cap \mathfrak{H}, \mathfrak{s}_r \cap \mathfrak{H}] \subset \mathfrak{s}_r \cap \mathfrak{H}$, and $[\mathfrak{u}_{r+1}, \mathfrak{s}_r \cap \mathfrak{N}] \subset \mathfrak{t}_r$ by (ii); hence $[X + T + U, U'] \in \mathfrak{t}_r$, and similarly $[U, X' + T'] \in \mathfrak{t}_r$. On p. 371, line 13, read $\tilde{x}^p$ instead of x^p. On p. 376, section 19, the field K has to be algebraically closed throughout. On p. 381, line 10 from bottom, read H^* instead of H. On p. 382, line 10, read "equal to C." In [10], p. 114, line 2, read [4] instead of [3]; in footnote 3, line 3, read $G_{n,m,r}$ instead of $G_{m,n}$. On p. 130, line 5, read $ms - j$ instead of $ms + j$.

the well-established cohomological notions which have proved their value in so many other theories. In our peculiar set-up, everything, of course, has first to be "formalized," in order to be able to do without set-theoretical concepts; but if this is done in the most trivial way for cross-sections (whose existence constitutes such a thorny problem in the case of algebraic groups), various technical difficulties arise in the extension of other basic concepts; I only mention here the absence of any sensible definition of 0-cochains (which is particularly troublesome for the low dimensional cohomology groups, in which we are especially interested), and the apparent necessity of introducing infinite-dimensional Lie groups as auxiliary tools, with all the extra care which is required when handling these somewhat elusive objects. Unfortunately, the so-called foundational books and papers on cohomology are, as usual, inadequate to cope with this new situation: they constitute at best a blueprint which one has to follow through endless tedious verifications, but do not provide any ready-made axiomatics which would dispense altogether with this unpleasant work; it is to be hoped that the more abstract homological algebra now in gestation in several quarters will fare better in this respect.

As a by-product of our investigation, it is, in particular, possible to give a complete description of all *two-dimensional* Lie groups over an algebraically closed field; apart from a satisfaction of mere curiosity, they provide unexpected counter-examples for several pleasant and plausible conjectures: for instance, an extension of the additive group by itself may very well be a non representable Lie group. This "pathology" seems to put strong limitations to the use of the theory of algebraic groups (as exemplified in [9]) to derive properties of formal Lie groups, and the unduly optimistic outlook expressed at the end of the introduction of [9] is no longer tenable.

2. Infinite dimensional formal Lie groups. It will be necessary for our purpose, to extend first the notion of formal Lie group to groups of "infinite dimension" in a manner which differs from the previous extensions of that type made in [6] and (by implication) in [8, no. 2]. Let I be an arbitrary set, and $\boldsymbol{x} = (x_i)_{i \in I}$ a set of indeterminates. When in the following we speak of a *power series* in the x_i with coefficients in a field K, we will *not* mean the most general power series in these indeterminates (as defined in [6, no. 2]), but only those series in which, for every integer $m \geqq 0$, there are only a *finite number of terms of total degree* $\leqq m$; these series obviously form a subalgebra of the algebra of all power series in the x_i, and it is *that* subalgebra which, by abuse of notation, we will write $K[[\boldsymbol{x}]]$ or $K[[x_i]]_{i \in I}$.

A fundamental consequence of that definition is that, if $(u_i)_{i\in I}$ is a family of elements of $K[[\mathbf{y}]]$ (where $\mathbf{y}=(y_j)_{j\in J}$), which are power series without constant terms, then it is possible to *substitute* the u_i to the x_i in any power series $v\in K[[\mathbf{x}]]$, and the resulting power series still belongs to $K[[\mathbf{y}]]$.

We can then define a formal Lie group of *dimension* $\mathrm{Card}(I)$ exactly as a formal Lie group of finite dimension, as well as the notion of homomorphism of a formal Lie group into another one (both of arbitrary dimension), by replacing power series in two sets of n indeterminates by power series (in the sense defined above) in two sets of indeterminates indexed by I, in the definitions given in [4, no. 2 and no. 3]. The existence of the "inverse" $\mathbf{x}^{-1}=(\theta_i(\mathbf{x}))$ in such a group G follows as in the finite dimensional case, the terms of total degree m in the power series θ_i being determined by induction on m. A similar argument proves the following

LEMMA 1. *Let (J,L) be an arbitrary partition of I. There exist two uniquely determined systems of power series without constant terms $\mathbf{u}(\mathbf{x})=(u_i(\mathbf{x}))_{i\in I}$ and $\mathbf{v}(\mathbf{x})=(v_i(\mathbf{x}))_{i\in I}$ such that $u_k(\mathbf{x})=0$ for $k\in L$, $v_j(\mathbf{x})=0$ for $j\in J$, and*

$$\mathbf{u}(\mathbf{x})\mathbf{v}(\mathbf{x})=\mathbf{x}. \tag{1}$$

Indeed, these conditions amount to the system of equations

$$u_j+\psi_j(\mathbf{u},\mathbf{v})=x_j \quad \text{for } j\in J,$$

$$v_k+\psi_k(\mathbf{u},\mathbf{v})=x_k \quad \text{for } k\in L,$$

where the ψ_i are power series all of whose terms have a total degree $\geqq 2$, and these have obviously a unique solution.

We observe that there is in general no hyperalgebra (in the usual sense, see for instance [8, no. 2]) corresponding to a formal Lie group of arbitrary dimension; this is due to the fact that if we write as usual $(\phi(\mathbf{x},\mathbf{y}))^\gamma=\sum_{\alpha,\beta} d_{\alpha\beta\gamma}\mathbf{x}^\alpha\mathbf{y}^\beta$, when α and β are given, there may well be an infinity of indices γ for which $d_{\alpha\beta\gamma}\neq 0$, hence the product of two left-invariant semi-derivations Z_α, Z_β on G will not in general be a finite linear combination of the Z_γ.

However, the main results which we shall need can be proved directly without the use of the hyperalgebras. If J is a subset of I, we say that J corresponds to a *typical subgroup* of G if the following condition is satisfied: for any system $(y_j)_{j\in J}=\mathbf{y}$ of indeterminates, define $\mathbf{j}(\mathbf{y})=(j_i(\mathbf{y}))$ as the system of power series $j_i(\mathbf{y})=y_i$ for $i\in J$, $j_i(\mathbf{y})=0$ otherwise; then we

must have $\phi_i(\boldsymbol{j}(\boldsymbol{y}), \boldsymbol{j}(\boldsymbol{z})) = 0$ for all indices $i \notin J$. If we write $\phi'_i(\boldsymbol{y}, \boldsymbol{z}) = \phi_i(\boldsymbol{j}(\boldsymbol{y}), \boldsymbol{j}(\boldsymbol{z}))$ for $i \in J$, the system of power series ϕ'_i defines a group law, and if we denote by H that formal Lie group, $\boldsymbol{j}$ is a homomorphism, which is called the natural injection of H into G. We say that H is a *normal* subgroup if the components of $\boldsymbol{x}\boldsymbol{j}(\boldsymbol{y})\boldsymbol{x}^{-1}$ of index $k \notin J$ are all 0; we can then write $\boldsymbol{x}\boldsymbol{j}(\boldsymbol{y})\boldsymbol{x}^{-1} = \boldsymbol{j}(\boldsymbol{u}(\boldsymbol{x}, \boldsymbol{y}))$, where $\boldsymbol{u}(\boldsymbol{x}, \boldsymbol{y}) = u_j(\boldsymbol{x}, \boldsymbol{y}))_{j \in J}$ is a system of power series without constant terms. When H is a normal typical subgroup of G, we now proceed to define the *quotient group* G/H. Using Lemma 1, there exist two well determined systems of power series $\boldsymbol{r}(\boldsymbol{x}) = (r_j(\boldsymbol{x}))_{j \in J}$ and $\boldsymbol{h}(\boldsymbol{x}) = (h_i(\boldsymbol{x}))_{i \in I}$ such that $h_i(\boldsymbol{x}) = 0$ for $i \in J$ and $\boldsymbol{x} = \boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))\boldsymbol{h}(\boldsymbol{x})$. If $\boldsymbol{y} = (y_i)$ is a second "generic point" of G, we can therefore write

$$\boldsymbol{x}\boldsymbol{y}^{-1} = \boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))\boldsymbol{h}(\boldsymbol{x})\boldsymbol{j}(\boldsymbol{r}(\boldsymbol{y}^{-1}))\boldsymbol{h}(\boldsymbol{y}^{-1}),$$

and using the fact that H is normal, this can also be written

$$\begin{aligned}\boldsymbol{x}\boldsymbol{y}^{-1} &= \boldsymbol{j}(\boldsymbol{u}^{(1)}(\boldsymbol{x}, \boldsymbol{y}))\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y}^{-1}) \\ &= \boldsymbol{j}(\boldsymbol{u}^{(2)}(\boldsymbol{x}, \boldsymbol{y}))\boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y}^{-1})),\end{aligned}$$

where $\boldsymbol{u}^{(1)}$ and $\boldsymbol{u}^{(2)}$ are systems of power series; hence, replacing $\boldsymbol{x}$ by $\boldsymbol{x}\boldsymbol{y}$ in that identity, we get

$$\boldsymbol{x} = \boldsymbol{j}(\boldsymbol{u}^{(2)}(\boldsymbol{x}\boldsymbol{y}, \boldsymbol{y}))\boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y})\boldsymbol{h}(\boldsymbol{y}^{-1})),$$

and from the uniqueness property of Lemma 1 (applied when K is replaced by a field containing $K[[\boldsymbol{y}]]$), we deduce

$$\boldsymbol{h}(\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y})\boldsymbol{h}(\boldsymbol{y}^{-1}));$$

finally, substituting $\boldsymbol{y}^{-1}$ to $\boldsymbol{y}$ in that identity, and then $\boldsymbol{x}\boldsymbol{y}$ to $\boldsymbol{x}$, we obtain

$$\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y}) = \boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y})). \tag{2}$$

For a system $\bar{\boldsymbol{x}} = (\bar{x}_k)_{k \in I-J}$ of indeterminates, let now $\sigma(\bar{\boldsymbol{x}})$ be the system $(\sigma_i(\bar{\boldsymbol{x}}))_{i \in I}$ of power series such that $\sigma_i(\bar{\boldsymbol{x}}) = 0$ for $i \in J$, $\sigma_i(\bar{\boldsymbol{x}}) = \bar{x}_i$ for $i \in I - J$; we claim that the system of power series $\Phi(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) = (\Phi_k(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}))_{k \in I-J}$ such that

$$\sigma(\Phi(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}})) = \boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}}))$$

defines a group law. Indeed, it is immediate that $\Phi(\bar{\boldsymbol{e}}, \bar{\boldsymbol{x}}) = \Phi(\bar{\boldsymbol{x}}, \bar{\boldsymbol{e}}) = \bar{\boldsymbol{x}}$, and from the definitions and from (2), we deduce that

$$\begin{aligned}\sigma(\Phi(\Phi(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}), \bar{\boldsymbol{z}})) &= \boldsymbol{h}(\sigma(\Phi(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}))\sigma(\bar{\boldsymbol{z}})) = \boldsymbol{h}(\boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}}))\boldsymbol{h}(\sigma(\bar{\boldsymbol{z}}))) \\ &= \boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}})\sigma(\bar{\boldsymbol{z}})),\end{aligned}$$

and a similar computation for $\sigma(\Phi(\bar{\boldsymbol{x}}, \Phi(\bar{\boldsymbol{y}}, \bar{\boldsymbol{z}})))$ proves the associativity condition. We will denote by G/H that formal Lie group and we will say that σ is the "typical" cross section of G/H; the system $\bar{\boldsymbol{h}}(\boldsymbol{x}) = (h_i(\boldsymbol{x}))_{i \in I-J}$ is then a homomorphism of G into G/H (called the natural homomorphism), and it is clear that $\bar{\boldsymbol{h}} \circ \boldsymbol{j} = 0$, $\bar{\boldsymbol{h}}(\sigma(\bar{\boldsymbol{x}})) = \bar{\boldsymbol{x}}$, and $\sigma(\bar{\boldsymbol{h}}(\boldsymbol{x})) = \boldsymbol{h}(\boldsymbol{x})$.

We may now define what we mean by an *exact sequence* of formal Lie groups and homomorphisms of the type

$$0 \to G' \xrightarrow{\boldsymbol{u}} G \xrightarrow{\boldsymbol{v}} G'' \to 0.$$

By definition, this means that there exist a formal Lie group G_1, a typical normal subgroup H_1 of G_1, and three isomorphisms $G' \to H_1$, $G \to G_1$, $G'' \to G_1/H_1$, such that the diagram

$$\begin{array}{ccccccccc} 0 & \to & G' & \xrightarrow{\boldsymbol{u}} & G & \xrightarrow{\boldsymbol{v}} & G'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & H_1 & \xrightarrow[\boldsymbol{j}]{} & G_1 & \xrightarrow[\bar{\boldsymbol{h}}]{} & G_1/H_1 & \to & 0 \end{array}$$

is commutative.

To go further, we should need the homomorphism theorem for formal Lie groups of arbitrary dimension; I do not know if such a theorem is valid in general. However, it will be enough, for our purposes, to consider homomorphisms $\boldsymbol{u}: G \to G'$ of a group G of *finite* dimension into an arbitrary formal Lie group G'. The proof of the homomorphism theorem given in [4, pp. 107-114] can then be transcribed *verbatim*, for all the "changes of variables" which intervene in that proof are defined by power series in the restricted sense which we have adopted at the beginning of this section. There exists therefore (when K is perfect) an isomorphism $G' \to G_1'$, and an isogeny $G \to H_1$ of G onto a typical subgroup of G_1', such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\boldsymbol{u}} & G' \\ \downarrow & & \downarrow \\ H_1 & \xrightarrow[\boldsymbol{j}]{} & G_1' \end{array}$$

is commutative.

3. Cohomology of formal Lie groups. We consider, on one hand, a formal Lie group G of *finite* dimension n over a perfect field K, and on the other hand, an *abelian* formal Lie group A over K, of arbitrary dimension; let I be the finite, J the arbitrary set of indices through which run the indices of the indeterminates defining the group laws of G and A respectively. A structure of *formal G-module* on A is defined by a system $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x}) = (f_j(\boldsymbol{s},\boldsymbol{x}))_{j\in J}$ of formal power series without constant terms and with coefficients in K, in the indeterminates s_i and x_j (with $\boldsymbol{s} = (s_i)$, $\boldsymbol{x} = (x_j)$, $i \in I$, $j \in J$); we write $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x}) = \boldsymbol{s}\cdot\boldsymbol{x}$, and we assume the following axioms:

$$\boldsymbol{s}\cdot(\boldsymbol{x}+\boldsymbol{y}) = \boldsymbol{s}\cdot\boldsymbol{x} + \boldsymbol{s}\cdot\boldsymbol{y} \tag{3}$$

($\boldsymbol{x},\boldsymbol{y}$ independent "generic points" of A, the group A being written additively; if $\boldsymbol{x}+\boldsymbol{y} = (\psi_j(\boldsymbol{x},\boldsymbol{y}))$ is the group law of A, (3), written in full, is the system of identities

$$f_j((s_i),(\psi_k(\boldsymbol{x},\boldsymbol{y}))) = \psi_j(\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x}),\boldsymbol{f}(\boldsymbol{s},\boldsymbol{y}))\,;$$

$$\boldsymbol{e}\cdot\boldsymbol{x} = \boldsymbol{x} \tag{4}$$

($\boldsymbol{e} = (0,\cdots,0)$, "neutral element" of G; this means of course that when the s_i are replaced by 0 in each f_j, the resulting series reduces to x_j);

$$\boldsymbol{s}\cdot(\boldsymbol{t}\cdot\boldsymbol{x}) = (\boldsymbol{s}\boldsymbol{t})\cdot\boldsymbol{x} \tag{5}$$

($\boldsymbol{s},\boldsymbol{t}$ independent "generic points" of G; this means here

$$f_j((s_i),(f_k(\boldsymbol{t},\boldsymbol{x}))) = f_j((\phi_i(\boldsymbol{s},\boldsymbol{t})),(x_k))$$

if $\boldsymbol{s}\boldsymbol{t} = (\phi_i(\boldsymbol{s},\boldsymbol{t}))$ is the group law of G). The usual properties of modules with coefficients in a group are "formalized" by following the same reasoning as in the classical case: for instance, if L is a field containing $K[[\boldsymbol{s}]]$, condition (3) means that $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x})$ is an endomorphism of the group $A_{(L)}$, and it follows from (4) and (5) that in fact it is an *automorphism* of that formal Lie group.

For each integer $m \geqq 1$, we now define a (non homogeneous) *m-cochain on G with values in A* as a system $\boldsymbol{g}(\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m) = (g_j(\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m))_{j\in J}$ of power series without constant terms and with coefficients in K, in m systems $\boldsymbol{s}_h = (s_{hi})_{i\in I}$ of n indeterminates ($1 \leqq h \leqq m$). We define the "sum" $\boldsymbol{g}+\boldsymbol{h}$ of two m-cochains $\boldsymbol{g} = (g_j)$, $\boldsymbol{h} = (h_j)$ as the system of power series in the s_{hi} obtained by substituting each g_j (resp. h_j) to x_j (resp. y_j) in each of the power series $\psi_j(\boldsymbol{x},\boldsymbol{y})$ defining the group law of A. It is then clear that for that "sum," the m-cochains on G with values in A form a (non

formal) abelian group $C^m(G,A)$. We next define the *coboundary operator* $d_{m+1}: C^m(G,A) \to C^{m+1}(G,A)$ by the usual formula

$$(6) \qquad d_{m+1}\boldsymbol{g}(s_1,\cdots,s_{m+1}) = s_1\cdot\boldsymbol{g}(s_2,\cdots,s_{m+1}) + \sum_{i=1}^{m}(-1)^i\boldsymbol{g}(s_1,\cdots,s_{i-1},s_is_{i+1},s_{i+2},\cdots,s_{m+1}) + (-1)^{m+1}\boldsymbol{g}(s_1,\cdots,s_m)$$

(the sum in the right hand side being taken according to the group law of A; and similarly, the minus signs denote inverses in A); the relation $d_{m+2}d_{m+1} = 0$, being purely formal, holds as in the classical case; the subgroup $Z^m(G,A) \subset C^m(G,A)$ of the *m-cocycles* is defined in the usual way for $m \geqq 1$, and the subgroup $B^m(G,A) \subset Z^m(G,A)$ of the *m-coboundaries* for $m \geqq 2$; hence the definition of the *m-th cohomology group*

$$H^m(G,A) = Z^m(G,A)/B^m(G,A)$$

for $m \geqq 2$. As there are no "elements" in A, there is no general definition of $B^1(G,A)$; however, when G operates *trivially* on A, i.e. when $s\cdot x = x$, we take, by definition, $B^1(G,A) = 0$, and then it is clear that $H^1(G,A) = Z^1(G,A)$ is the group of *homomorphisms* of G into A.

Let B be a second formal G-module, and $\boldsymbol{u} = (u_k)$ a *homomorphism* of A into B, i.e. a homomorphism of the abelian group A into the abelian group B such that $\boldsymbol{u}(s\cdot x) = s\cdot\boldsymbol{u}(x)$; for each m-cochain $\boldsymbol{g} \in C^m(G,A)$, the system

$$(\boldsymbol{u}\circ\boldsymbol{g})(s_1,\cdots,s_m) = (u_k(\boldsymbol{g}(s_1,\cdots,s_m)))$$

of power series is an m-cochain $\boldsymbol{u}\circ\boldsymbol{g} \in C^m(G,B)$; due to (6) and to the relation $\boldsymbol{u}(s\cdot x) = s\cdot\boldsymbol{u}(x)$, it is immediately verified that $\boldsymbol{u}\circ\boldsymbol{g}$ is a cocycle (resp. a coboundary) when $\boldsymbol{g}$ is a cocycle (resp. a coboundary). Hence the mapping $u: \boldsymbol{g} \to \boldsymbol{u}\circ\boldsymbol{g}$ defines a homomorphism u^* of $H^m(G,A)$ into $H^m(G,B)$ for $m \geqq 2$ (and also for $m = 1$ when G acts trivially on A and on B). Furthermore, it is obvious from the definitions that if C is a third formal G-module, $\boldsymbol{v}$ a homomorphism of B into C, and $\boldsymbol{w} = \boldsymbol{v}\circ\boldsymbol{u}$, we have for the corresponding homomorphisms, $w^* = v^*\circ u^*$. This implies, in particular, that when A and B are isomorphic formal G-modules, $H^m(G,A)$ and $H^m(G,B)$ are isomorphic.

Consider now a G-module B, and a typical subgroup A of B, corresponding to a subset L of the set J of indices corresponding to B. We say that A is a *submodule* of B if A is a G-module and if, for the natural injection $\boldsymbol{j}$ of A into B, we have $\boldsymbol{j}(s\cdot y) = s\cdot\boldsymbol{j}(y)$ (y generic point of A).

It is then possible to define on B/A a structure of G-module in the following way: with the notations of Section 2 (except that the group law of B is now written additively), we have

$$\begin{aligned} \boldsymbol{s}\cdot\boldsymbol{x} &= \boldsymbol{s}\cdot(\boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))) + \boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x}) \\ &= \boldsymbol{j}(\boldsymbol{s}\cdot\boldsymbol{r}(\boldsymbol{x})) + \boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x}) \\ &= \boldsymbol{j}(\boldsymbol{v}(\boldsymbol{x})) + \boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x})), \end{aligned}$$

where $\boldsymbol{v}$ is some system of power series; the uniqueness property of Lemma 1 implies

$$\boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x})). \tag{7}$$

It is then an easy matter to verify, using (7) and (2) and the definition of the group law in B/A, that, if we define $\boldsymbol{s}\cdot\bar{\boldsymbol{x}}$ as the system of power series such that $\sigma(\boldsymbol{s}\cdot\bar{\boldsymbol{x}}) = \boldsymbol{h}(\boldsymbol{s}\cdot\sigma(\bar{\boldsymbol{x}}))$, the axioms (3) to (5) are satisfied, and that the natural homomorphism $\bar{\boldsymbol{h}}$ of B onto B/A is a homomorphism of G-modules.

We then extend the definition of an *exact sequence* of G-modules

$$0 \to A \xrightarrow{\boldsymbol{i}} B \xrightarrow{\boldsymbol{p}} C \to 0$$

by requesting that, in the corresponding definition given in Section 2 for groups, all the groups are G-modules and all homomorphisms are homomorphisms of G-modules.[2] With that definition, we can verify immediately that the corresponding sequence of (non formal) abelian groups and homomorphisms

$$0 \to C^m(G,A) \xrightarrow{i} C^m(G,B) \xrightarrow{p} C^m(G,C) \to 0$$

is *exact*: we can namely suppose first that A is a typical submodule of B, C the quotient module B/A, and that $\boldsymbol{i}$ and $\boldsymbol{p}$ are the natural homomorphisms $\boldsymbol{j}$ and $\bar{\boldsymbol{h}}$. Suppose that $\boldsymbol{g}$ is an m-cochain in $C^m(G,B)$ such that $\bar{\boldsymbol{h}}\circ\boldsymbol{g} = 0$; using Lemma 1, we can write

$$\boldsymbol{g} = \boldsymbol{j}\circ\boldsymbol{g}_1 + \sigma\circ\boldsymbol{g}_2,$$

where $\boldsymbol{g}_1 \in C^m(G,A)$ and $\boldsymbol{g}_2 \in C^m(G,B)$; the assumption means that $\sigma\circ\boldsymbol{g}_2 = 0$, hence our conclusion.

The general methods of cohomology can then be applied to define homo-

[2] The field K has here arbitrary characteristic, and there can be no confusion between the meaning of the letter $\boldsymbol{p}$ here and its usual meaning (Frobenius homomorphism) in groups over a field of characteristic p.

morphisms $\partial: H^m(G,C) \to H^{m+1}(G,A)$ for $m \geqq 2$, and to prove that the sequence

$$(8)\quad H^2(G,A) \xrightarrow{i^*} H^2(G,B) \xrightarrow{p^*} H^2(G,C) \xrightarrow{\partial} H^3(G,A) \to \cdots$$

$$\cdots \to H^m(G,A) \xrightarrow{i^*} H^m(G,B) \xrightarrow{p^*} H^m(G,C) \xrightarrow{\partial} H^{m+1}(G,A) \to \cdots$$

is *exact* ("exact sequence of cohomology"); furthermore, when G operates trivially on A, B and C, the sequence can begin with $H^1(G,A)$, as is readily verified. Finally, suppose we have two exact sequence of G-modules, connected by homomorphisms

$$\begin{array}{ccccccccc} 0 & \to & A & \longrightarrow & B & \longrightarrow & C & \to & 0 \\ & & \boldsymbol{u}\downarrow & & \boldsymbol{v}\downarrow & & \boldsymbol{w}\downarrow & & \\ 0 & \to & A' & \longrightarrow & B' & \longrightarrow & C' & \to & 0 \end{array}$$

such that the diagram is commutative; it is then clear that the corresponding diagram for m-cochains

$$\begin{array}{ccccccccc} 0 & \to & C^m(G,A) & \longrightarrow & C^m(G,B) & \longrightarrow & C^m(G,C) & \to & 0 \\ & & u\downarrow & & v\downarrow & & w\downarrow & & \\ 0 & \to & C^m(G,A') & \longrightarrow & C^m(G,B') & \longrightarrow & C^m(G,C') & \to & 0 \end{array}$$

is commutative, and then the general methods of cohomology prove that the diagram

$$\begin{array}{ccccccccccc} \cdots & \to & H^m(G,A) & \longrightarrow & H^m(G,B) & \longrightarrow & H^m(G,C) & \longrightarrow & H^{m+1}(G,A) & \to & \cdots \\ & & u^*\downarrow & & v^*\downarrow & & w^*\downarrow & & u^*\downarrow & & \\ \cdots & \to & H^m(G,A') & \longrightarrow & H^m(G,B') & \longrightarrow & H^m(G,C') & \longrightarrow & H^{m+1}(G,A') & \to & \cdots \end{array}$$

is also commutative.

4. The Hochschild-Serre exact sequence.[3] Let $\boldsymbol{u}$ be a homomorphism of a formal Lie group H (of finite dimension) into G. It is immediate that

[3] The result which we prove in this section is the extension to our situation of a very special corollary of the results of Hochschild and Serre [11]; they use very heavy homological machinery, and the labor of extending that machinery to the present case would (if possible at all) be out of proportion to our needs. The "elementary" proof which I follow here is patterned after a similar proof for the classical case, which was kindly communicated to me by G. Hochschild.

if A is a G-module, A is made into an H-module if we define $\boldsymbol{t} \cdot \boldsymbol{x}$ as equal to $\boldsymbol{u}(\boldsymbol{t}) \cdot \boldsymbol{x}$ for a "generic point" $\boldsymbol{t}$ of H. If $\boldsymbol{g}$ is any cochain in $C^m(G, A)$, then $\boldsymbol{g}'(\boldsymbol{t}_1, \cdots, \boldsymbol{t}_m) = \boldsymbol{g}(\boldsymbol{u}(\boldsymbol{t}_1), \cdots, \boldsymbol{u}(\boldsymbol{t}_m))$ is an m-cochain in $C^m(H, A)$; if we denote it by $\bar{u}(\boldsymbol{g})$, $\bar{u}$ is a homomorphism of $C^m(G, A)$ into $C^m(H, A)$, and formula (6) shows that $\bar{u}$ commutes with d_{m+1}. Hence, for $m \geqq 2$, we have a homomorphism

$$u^* : H^m(G, A) \to H^m(H, A);$$

when G operates trivially on A, so does H, and the definition of u^* can be extended for $m = 1$. Furthermore, it is readily verified that, for any exact sequence $0 \to A \to B \to C \to 0$ of G-modules, the diagram

$$\begin{array}{ccccccccc}
\cdots \to H^m(G, A) & \longrightarrow & H^m(G, B) & \longrightarrow & H^m(G, C) & \longrightarrow & H^{m+1}(G, A) \to \cdots \\
\Big\downarrow u^* & & \Big\downarrow u^* & & \Big\downarrow u^* & & \Big\downarrow u^* & & \\
\cdots \to H^m(H, A) & \longrightarrow & H^m(H, B) & \longrightarrow & H^m(H, C) & \longrightarrow & H^{m+1}(H, A) \to \cdots
\end{array}$$

is commutative.

From now on, we shall suppose that the G-module A has *finite* dimension. We introduce, after A. Weil (cf. [11, p. 114, Cor. to Prop. 3]), a new formal abelian group $M(G, A)$ of infinite dimension, corresponding to the set of indices $L = J \times \mathbf{N}^l$; for two "generic points" $\boldsymbol{u} = (u_{j\alpha})$, $\boldsymbol{v} = (v_{j\alpha})$, the composition law $\boldsymbol{w} = \boldsymbol{u} + \boldsymbol{v}$ is defined in the following way. We associate to $\boldsymbol{u}$ and to a "generic point" $\boldsymbol{s}$ of G the system of power series which we write $\boldsymbol{u}(\boldsymbol{s}) = (u_j(\boldsymbol{s}))$ in the $u_{j\alpha}$ and s_i, such that $u_j(\boldsymbol{s}) = \sum_{\alpha} u_{j\alpha} \boldsymbol{s}^{\alpha}$ (note that these series have no constant term, but each one has a unique term which does not contain any s_i, namely u_{j0}); the mapping $\boldsymbol{u} \to \boldsymbol{u}(\boldsymbol{s})$ is of course bijective; $\boldsymbol{w}$ is then defined by the condition $\boldsymbol{w}(\boldsymbol{s}) = \boldsymbol{u}(\boldsymbol{s}) + \boldsymbol{v}(\boldsymbol{s})$ (sum taken for the group law of A), and it is immediately verified that $w_{j\alpha}$ is actually a *polynomial* in the $u_{j\alpha}$ and $v_{j\alpha}$; the associativity and commutativity of the group law are obvious. We next make $M(G, A)$ into a G-module by the definition $(\boldsymbol{s} \cdot \boldsymbol{u})(\boldsymbol{s}') = \boldsymbol{u}(\boldsymbol{s}'\boldsymbol{s})$ ($\boldsymbol{s}, \boldsymbol{s}'$ independent generic points of G); if we write as usual $(\boldsymbol{s}'\boldsymbol{s})^{\gamma} = \sum_{\alpha,\beta} d_{\alpha\beta\gamma} \boldsymbol{s}'^{\alpha} \boldsymbol{s}^{\beta}$, we have therefore, for $\boldsymbol{v} = \boldsymbol{s} \cdot \boldsymbol{u}$, $v_{j\alpha} = \sum_{\beta,\gamma} d_{\alpha\beta\gamma} u_{j\gamma} \boldsymbol{s}^{\beta}$, and as G has finite dimension, there are only a finite number of $d_{\alpha\beta\gamma}$ which are $\neq 0$ for given α and β, which shows that the power series defining $\boldsymbol{s} \cdot \boldsymbol{u}$ are of the type allowed by our conventions; the verification of axioms (3), (4) and (5) is then immediate. Observe in passing that for the definition of the structure of G-module on $M(G, A)$,

the structure of G-module of A is irrelevant, only its structure of abelian group intervenes.

It is immediate from the definitions that for any m-cochain $\boldsymbol{f}$ in $C^m(G, M)$, $\boldsymbol{f}_*(\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_m) = \boldsymbol{f}(\boldsymbol{s}_1, \cdots, \boldsymbol{s}_m)(\boldsymbol{s}_0)$ is an $(m+1)$-cochain in $C^{m+1}(G, A)$, and $\boldsymbol{f} \to \boldsymbol{f}_*$ is an isomorphism of $C^m(G, M)$ onto $C^{m+1}(G, A)$. Moreover, we can here define 1-coboundaries in $C^1(G, M)$ as the 1-cochains $\boldsymbol{f}$ such that $\boldsymbol{f}_*(\boldsymbol{s}_0, \boldsymbol{s}_1) = \boldsymbol{g}(\boldsymbol{s}_0\boldsymbol{s}_1) - \boldsymbol{g}(\boldsymbol{s}_0)$, where $\boldsymbol{g}$ is a 1-cochain in $C^1(G, A)$. For any subgroup H of G, $M(G, A)$ is also an H-module, and the cochains in $C^m(H, M)$ correspond now to the systems of power series $\boldsymbol{f}_*(\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_m)$, where $\boldsymbol{s}_0$ is a generic point of G, $\boldsymbol{s}_1, \cdots, \boldsymbol{s}_m$ independent generic points of H; 1-coboundaries are again defined in the same way. With these definitions:

LEMMA 2. *For any subgroup H of G, $H^m(H, M(G, A)) = 0$ for any $m \geqq 1$.*

Indeed, if we write that an m-cochain $\boldsymbol{f} \in C^m(H, M)$ is such that $d_{m+1}\boldsymbol{f} = 0$, we obtain, from formula (6)

$$\boldsymbol{f}_*(\boldsymbol{s}_0\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_{m+1}) + \sum_{i=1}^{m} (-1)^i \boldsymbol{f}_*(\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_i\boldsymbol{s}_{i+1}, \cdots, \boldsymbol{s}_{m+1}) + (-1)^{m+1}\boldsymbol{f}_*(\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_m) = 0. \tag{9}$$

when $\boldsymbol{s}_0$ is a generic point of G, the $\boldsymbol{s}_i$ $(i \geqq 1)$ independent generic points of H. We may obviously suppose the subgroup H is typical, defined, for instance, by the relations $s_i = 0$ for $i \in I - I_0$. Using Lemma 1, we can therefore write for a generic point $\boldsymbol{s}$ of G, $\boldsymbol{s} = \boldsymbol{h}(\boldsymbol{s})\boldsymbol{r}(\boldsymbol{s})$, where $h_i(\boldsymbol{s}) = 0$ for $i \in I_0$, $r_i(\boldsymbol{s}) = 0$ for $i \in I - I_0$; if $\boldsymbol{t}$ is a generic point of H, we have $\boldsymbol{h}(\boldsymbol{t}) = \boldsymbol{e}$, $\boldsymbol{r}(\boldsymbol{t}) = \boldsymbol{t}$; using these results and the uniqueness property of Lemma 1, it is easy to verify, as in Section 2, that $\boldsymbol{h}(\boldsymbol{st}) = \boldsymbol{h}(\boldsymbol{s})$ and $\boldsymbol{r}(\boldsymbol{st}) = \boldsymbol{r}(\boldsymbol{s})\boldsymbol{t}$. Consider now the system of power series

$$\boldsymbol{g}_*(\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_{m-1}) = \boldsymbol{f}_*(\boldsymbol{h}(\boldsymbol{s}_0), \boldsymbol{r}(\boldsymbol{s}_0), \boldsymbol{s}_1, \cdots, \boldsymbol{s}_{m-1})$$

with the same assumptions on the $\boldsymbol{s}_i$; formula (9) and the preceding properties of $\boldsymbol{h}$ and $\boldsymbol{r}$ show at once that $\boldsymbol{f} = d_m\boldsymbol{g}$, hence our result (the case $m = 1$ has, of course, to be considered separately, since we have not defined 0-cochains, but directly 1-coboundaries).

We next introduce the *lift* mapping. Let P be a G-module (of finite or infinite dimension), and let H be a *normal* subgroup of G; suppose in addition that the relations $\boldsymbol{t} \cdot \boldsymbol{x} = \boldsymbol{x}$, for a generic point $\boldsymbol{t}$ of H, "define" a subgroup P^H of P (this means that, after a suitable "change of variables" in P, the equations obtained by writing that in the power series $f_j(\boldsymbol{t}, \boldsymbol{x})$,

considered as series in the t_i, the coefficients are all zero except the terms independent of $\boldsymbol{t}$, form a system equivalent to the system obtained by equating to 0 a subset of the indeterminates x_j). Then, if $\boldsymbol{y}$ is a generic point of P^H, we have $(\boldsymbol{ts})\cdot\boldsymbol{y} = \boldsymbol{s}\cdot\boldsymbol{y}$ for a generic point $\boldsymbol{s}$ of G, since H is normal in G; therefore P^H is a G-submodule. We may suppose that H is a typical normal subgroup of G, and keep the notations of Lemma 2. For a system of indeterminates $\bar{\boldsymbol{s}} = (\bar{s}_k)_{k\in I-I_0}$, we define $\sigma(\bar{\boldsymbol{s}}) = (\sigma_i(\bar{\boldsymbol{s}}))$ such that $\sigma_i(\bar{\boldsymbol{s}}) = 0$ for $i \in I_0$, $\sigma_i(\bar{\boldsymbol{s}}) = \bar{s}_i$ for $i \in I - I_0$; it is readily verified that $\bar{\boldsymbol{s}}\cdot\boldsymbol{y} = \sigma(\bar{\boldsymbol{s}})\cdot\boldsymbol{y}$ defines a structure of (G/H)-module on P^H, and that the original structure of G-module on P^H is obtained by the process described at the beginning of this section applied to the natural homomorphism $\bar{\boldsymbol{h}}$ of G into G/H. If we designate by $\boldsymbol{i}$ the natural injection $P^H \to P$, we obtain therefore a homomorphism

$$\lambda : H^m(G/H, P^H) \xrightarrow{\bar{h}^*} H^m(G, P^H) \xrightarrow{i^*} H^m(G, P)$$

$(m \geqq 2)$, which we call the *lift* mapping.

It can also be described as deriving (by passage to quotients) from the mapping

$$\lambda : C^m(G/H, P^H) \to C^m(G, P)$$

which to each cochain $\boldsymbol{g}(\bar{\boldsymbol{s}}_1, \cdots, \bar{\boldsymbol{s}}_m)$ in $C^m(G/H, P^H)$, associates the cochain $\boldsymbol{i}(\boldsymbol{g}(\bar{\boldsymbol{h}}(\boldsymbol{s}_1), \cdots, \bar{\boldsymbol{h}}(\boldsymbol{s}_m)))$ in $C^m(G, P)$.

We can now state and prove the main result of this section:

PROPOSITION 1. *Suppose A is an abelian Lie group of finite dimension, on which G operates trivially, and that H is a normal subgroup of G such that $H^1(H_{(N)}, A_{(N)}) = 0$ for any extension N of the field K. Then the sequence*

$$0 \to H^2(G/H, A) \xrightarrow{\lambda^*} H^2(G, A) \xrightarrow{\rho^*} H^2(H, A)$$

(ρ natural injection of H into G) is exact.

We introduce, as above, the G-module $M(G, A) = M$, and we consider in addition the mapping $\boldsymbol{j} : A \to M$ such that $j_{k0}(\boldsymbol{x}) = x_k$, $j_{k\alpha}(\boldsymbol{x}) = 0$ whenever $\alpha \neq 0$ $(k \in J)$ (in other words, $\boldsymbol{j}(\boldsymbol{x})(\boldsymbol{s}) = (j_k(\boldsymbol{x}, \boldsymbol{s}))$ is the system of power series $j_k(\boldsymbol{x}, \boldsymbol{s}) = x_k$). As G operates trivially on A, $\boldsymbol{j}$ is a homomorphism of G-modules; homeover $\boldsymbol{j}(A)$ is the typical subgroup of M defined by the relations $u_{k\alpha} = 0$ for $\alpha \in J$ and $\alpha \neq 0$. We may therefore consider the quotient G-module $C = M/\boldsymbol{j}(A)$; we shall denote by $\boldsymbol{p}$ the natural homomorphism of M into C; we have by definition $\boldsymbol{s}\cdot\boldsymbol{p}(\boldsymbol{u}) = \boldsymbol{p}(\boldsymbol{s}\cdot\boldsymbol{u})$.

From that definition, it follows that for any m-cochain $\boldsymbol{f}$ in $C^m(G,C)$, $\tau(\boldsymbol{f}(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_m))(\boldsymbol{s}_0)=\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)$ (τ typical cross section of $M/\boldsymbol{j}(A)$) is a system of power series in which there are no terms independent of $\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m$, i.e. such that $\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{e},\cdots,\boldsymbol{e})=0$. We observe that the 1-coboundaries in $C^1(G,M)$, as defined above, have that property, and by definition, we take these 1-cochains as 1-coboundaries in $C^1(G,C)$; the cochains in $C^m(H,C)$ and the 1-coboundaries in $C^1(H,C)$ are characterized in the same way.

We now proceed to show that M^H and C^H are "defined" in the sense described above, and to characterize these submodules. The relation $\boldsymbol{t}\cdot\boldsymbol{u}=\boldsymbol{u}$ means $\boldsymbol{u}(\boldsymbol{st})=\boldsymbol{u}(\boldsymbol{s})$ ($\boldsymbol{s}$ generic point of G, $\boldsymbol{t}$ generic point of H); using the notations introduced in Lemma 2, this implies $\boldsymbol{u}(\boldsymbol{s})=\boldsymbol{u}(\boldsymbol{h}(\boldsymbol{s})\boldsymbol{r}(\boldsymbol{s}))=\boldsymbol{u}(\boldsymbol{h}(\boldsymbol{s}))$; conversely, for any system $\boldsymbol{v}=(v_{k\alpha})$ of indeterminates, $\boldsymbol{u}(\boldsymbol{s})=\boldsymbol{v}(\boldsymbol{h}(\boldsymbol{s}))$ is such that $\boldsymbol{u}(\boldsymbol{st})=\boldsymbol{u}(\boldsymbol{s})$. If we remember that $h_i(\boldsymbol{s})=0$ for $i\in I_0$, $h_i(\boldsymbol{s})=s_i+\cdots$ (unwritten terms of degree $\geqq 2$) for $i\in I-I_0$, it follows easily, by induction on $|\alpha|$, that the relation $\boldsymbol{t}\cdot\boldsymbol{u}=\boldsymbol{u}$ is equivalent to an infinite system of equations of the following type: $u_{k,\epsilon_i}=0$ for $i\in I_0$, and, for any index $\alpha=(\alpha_1,\cdots,\alpha_n)$ such that $|\alpha|>1$ and one at least of the α_i for $i\in I_0$ is $\neq 0$,

$$u_{k\alpha}=P_{k\alpha}((u_{j\beta})) \qquad (k\in J),$$

where $P_{k\alpha}$ is a polynomial with integral coefficients in the $u_{j\beta}$ ($j\in J$) such that $|\beta|<|\alpha|$ and all non-zero components of β have their index in $I-I_0$. The "change of variables" $u'_{k\alpha}=u_{k\alpha}-P_{k\alpha}((u_{j\beta}))$ for all indices α such that at least one α_i for $i\in I_0$ is $\neq 0$ (with $P_{k\alpha}=0$ if $|\alpha|=1$) reduces M^H to a typical subgroup. This shows further that the mapping $\boldsymbol{v}\to\boldsymbol{v}\circ\bar{\boldsymbol{h}}$ is an isomorphism of the abelian group $M(G/H,A)$ onto M^H; moreover, if $\bar{\boldsymbol{s}}'$ is a generic point of G/H, we have

$$\begin{aligned}(\bar{\boldsymbol{s}}'\cdot\boldsymbol{v})(\bar{\boldsymbol{h}}(\boldsymbol{s}))&=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s})\bar{\boldsymbol{s}}')=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s})\bar{\boldsymbol{h}}(\sigma(\bar{\boldsymbol{s}}')))\\&=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s}\sigma(\bar{\boldsymbol{s}}')))=(\sigma(\bar{\boldsymbol{s}}')\cdot(\boldsymbol{v}\circ\bar{\boldsymbol{h}}))(\boldsymbol{s})\end{aligned}$$

which proves that the preceding isomorphism is also an isomorphism of (G/H)-modules. We deduce therefore from Lemma 2 that $H^m(G/H,M^H)=0$ for any $m\geqq 1$.

Our next step is to prove that, due to the relation $H^1(H_{(N)},A_{(N)})=0$, the sequence $0\to A\xrightarrow{\boldsymbol{j}}M^H\xrightarrow{\boldsymbol{p}^H}C^H\to 0$ (where $\boldsymbol{p}^H$ is the restriction of $\boldsymbol{p}$ to M^H) is *exact*. If $\bar{\boldsymbol{u}}$ is a generic point of C, the condition $\boldsymbol{t}\cdot\bar{\boldsymbol{u}}=\bar{\boldsymbol{u}}$ which defines C^H is equivalent to $\boldsymbol{p}(\boldsymbol{t}\cdot\tau(\bar{\boldsymbol{u}})-\tau(\bar{\boldsymbol{u}}))=0$; the components of $\tau(\bar{\boldsymbol{u}})$

are $\tau_{k0}(\bar{\boldsymbol{u}}) = 0$ for $k \in J$ and $\tau_{k\alpha}(\bar{\boldsymbol{u}}) = \bar{u}_{k\alpha}$ for $\alpha \neq 0$, $k \in J$; if we write $\boldsymbol{w} = \tau(\bar{\boldsymbol{u}})$ for simplicity's sake, the relation $\boldsymbol{t} \cdot \bar{\boldsymbol{u}} = \bar{\boldsymbol{u}}$ means that the power series of the system $\boldsymbol{w}(\boldsymbol{st}) - \boldsymbol{w}(\boldsymbol{s})$ (considered as power series in the s_i) have all their coefficients 0 except the constant terms (which are power series in the t_i $(i \in I_0)$ and the $\bar{u}_{k\alpha}$); as $\boldsymbol{w}(\boldsymbol{e}) = 0$, we have therefore

$$\boldsymbol{w}(\boldsymbol{st}) - \boldsymbol{w}(\boldsymbol{s}) = \boldsymbol{w}(\boldsymbol{t}).$$

From this relation it follows, in particular, if $\boldsymbol{t}'$ is a second generic point of H, that $\boldsymbol{w}(\boldsymbol{t}'\boldsymbol{t}) = \boldsymbol{w}(\boldsymbol{t}') + \boldsymbol{w}(\boldsymbol{t})$; if N is a field containing $K[[\bar{\boldsymbol{u}}]]$, this means that the system of power series $\boldsymbol{w}(\boldsymbol{t})$ over N is a homomorphism of $H_{(N)}$ into $A_{(N)}$. Our assumption implies that $\boldsymbol{w}(\boldsymbol{t}) = 0$, hence $\boldsymbol{w}(\boldsymbol{st}) = \boldsymbol{w}(\boldsymbol{s})$; in other words, the relation $\boldsymbol{t} \cdot \bar{\boldsymbol{u}} = \bar{\boldsymbol{u}}$ implies that $\tau(\bar{\boldsymbol{u}})$ verifies the condition which defines M^H, and the converse is obvious, which proves our assertion.

We may observe here that the relations $u_{k0} = 0$ $(k \in J)$ also define a subgroup in M, and τ is an isomorphism of C onto that subgroup; similarly, when M^H is identified with $M(G/H, A)$, τ, restricted to C^H, is an isomorphism of that group onto the subgroup of $M(G/H, A)$ defined in a similar way. In particular, we see that the 1-cochains in $C^1(G/H, C^H)$ are identified to systems $\boldsymbol{f}_*(\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{s}}_1)$ ($\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{s}}_1$ independent generic points in G/H) such that $\boldsymbol{f}_*(\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{e}}) = 0$, and the 1-coboundaries in $C^1(G/H, C^H)$ can again be identified with the 1-coboundaries in $C^1(G/H, M^H)$. The 1-coboundaries in $C^1(G, C)$ (resp. $C^1(G/H. C^H)$) are thus the images by p (resp. p^H) of the 1-coboundaries in $C(G, M)$ (resp. $C^1(G/H, M^H)$). It is then a routine matter to verify that these remarks allow us to define the homomorphisms ∂ in the horizontal lines of the following diagram, and to prove that these lines are exact sequences:

(10)

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & \overset{\partial}{\nearrow} & \downarrow & & \\
0 = H^1(G/H, M^H) & \to & H^1(G/H, C^H) & \longrightarrow & H^2(G/H, A) & \to & H^2(G/H, M^H) = 0 \\
 & & \downarrow \lambda^* & & \downarrow \lambda^* & & \\
 & & & \overset{\partial}{\nearrow} & & & \\
0 = H^1(G, M) & \to & H^1(G, C) & \longrightarrow & H^2(G, A) & \to & H^2(G, M) = 0 \\
 & & \downarrow \rho^* & & \downarrow \rho^* & & \\
 & & & \overset{\partial}{\nearrow} & & & \\
0 = H^1(K, M) & \to & H^1(K, C) & \longrightarrow & H^2(K, A) & \to & H^2(K, M) = 0
\end{array}$$

The second vertical line has already been defined, but we still have to define the first vertical line and to prove that the diagram (10) is commutative. If a cochain $\boldsymbol{f}$ in $C^1(G/H, C^H)$ is identified to the system of power series

$f_*(\tilde{s}_0, \tilde{s}_1)$ (such that $f_*(\tilde{s}_0, \tilde{e}) = 0$), $\lambda(f)$ is by definition the cochain associated to the system $f_*(\bar{h}(s_0), \bar{h}(s_1))$. From the definitions, it follows that $\lambda(\tilde{s} \cdot f)$ is equal to $\sigma(\tilde{s}) \cdot \lambda(f)$; hence, if f is a cocycle, so is $\lambda(f)$; furthermore, the definitions given above show that if f is a 1-coboundary, so is $\lambda(f)$, hence the definition of λ^*: $H^1(G/H, C^H) \to H^1(G, C)$. In addition, if f is a cocycle belonging to the cohomology class c, the class ∂c contains the 2-cocycle $f_*(\tilde{s}_0, \tilde{s}_1) - f_*(\tilde{e}, \tilde{s}_0\tilde{s}_1) + f_*(\tilde{e}, \tilde{s}_0)$, as is immediate from the definition of ∂; a similar computation for $\partial(\lambda^*(c))$ proves the commutativity in the two first horizontal lines of the diagram. The definition of ρ^* and the verification of the commutativity in the last two horizontal lines are even simpler and we omit them.

We have used Lemma 2 to replace the left and right extremities of the horizontal lines in (10) by 0; to end the proof of Proposition 1, it remains therefore to prove that the first vertical line is an exact sequence. We first show that λ^* is injective. With the same notations as above, suppose $\lambda(f)$ is a coboundary; this means that $f_*(\bar{h}(s_0), \bar{h}(s_1)) = g(s_0 s_1) - g(s_0)$; but if t is a generic point of H, $\bar{h}(s_1 t) = \bar{h}(s_1)$, hence $g(s_0 s_1 t) = g(s_0 s_1)$; replacing s_0 by e, s_1 by $h(s)$, t by $r(s)$ (s generic point of G; notations of Lemma 2), we get $g(s) = g(h(s)) = g(\sigma(\bar{h}(s)))$, and therefore f is a coboundary.

Finally, it is clear that $\rho^*\lambda^* = 0$, and we have only to show that any element in the kernel of ρ^* is in the image of λ^*. Let therefore f be a cocycle in $C^1(G, C)$ such that the image by ρ^* of its cohomology class is 0. This means that $f_*(s_0, s_1)$ is such that, for a generic point t of H, $f_*(s_0, t) = g(s_0 t) - g(s_0)$. Using equation (9) (for $m = 1$), we get

$$f_*(s_0, s_1 t) = f_*(s_0 s_1, t) + f_*(s_0, s_1) = f_*(s_0, s_1) + g(s_0 s_1 t) - g(s_0 s_1).$$

Let $f'_*(s_0, s_1) = f_*(s_0, s_1) - g(s_0 s_1) + g(s_0)$; then f' is obviously a cocycle which is cohomologous to f, and we have

$$f'_*(s_0, s_1 t) = f'_*(s_0, s_1). \tag{11}$$

As $t s_1 = s_1(s_1^{-1} t s_1)$, and H is normal, (11) also implies

$$f'_*(s_0, t s_1) = f'_*(s_0, s_1); \tag{12}$$

on the other hand, equation (9) yields

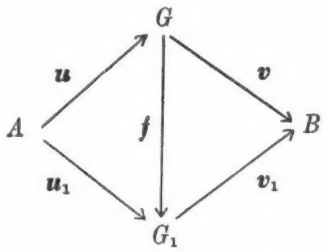
$$f'_*(s_0 t, s_1) - f'_*(s_0, t s_1) + f'_*(s_0, t) = 0,$$

and we have, by assumption, $f'_*(s_0, t) = 0$, hence

$$f'_*(s_0 t, s_1) = f'_*(s_0, s_1). \tag{13}$$

Equations (11) and (13) show that, if $f''_*(\bar{s}_0, \bar{s}_1) = f'_*(\sigma(\bar{s}_0), \sigma(\bar{s}_1))$, f'' is a cocycle in $C^1(G/H, C^H)$ and that $f' = \lambda f''$); the proof of Proposition 1 is thus complete.

5. Group extensions and cohomology. Let A, B be two formal Lie groups of finite dimension over a perfect field K. We say that a formal Lie group G over K and a pair of homomorphisms $A \xrightarrow{\boldsymbol{u}} G \xrightarrow{\boldsymbol{v}} B$ constitute an *extension of B by A* if $\boldsymbol{u}$ is a monomorphism, $\boldsymbol{v}$ an epimorphism and if the kernel of $\boldsymbol{v}$ is equal to the image of $\boldsymbol{u}$; B is then isomorphic to $G/\boldsymbol{u}(A)$. We say, as usual, that two extensions $(G, \boldsymbol{u}, \boldsymbol{v})$, $(G_1, \boldsymbol{u}_1, \boldsymbol{v}_1)$ are *equivalent* if there exists an isomorphism $\boldsymbol{f}: G \to G_1$ such that the diagram



is commutative. If α is an isomorphism of K onto a field K', and if we denote by A^α, B^α, G^α, $\boldsymbol{u}^\alpha$, $\boldsymbol{v}^\alpha$ the groups and homomorphisms obtained by applying to all coefficients of the series defining A, B, G, $\boldsymbol{u}$, $\boldsymbol{v}$ the isomorphism α, it is clear from the definitions that $A^\alpha \xrightarrow{\boldsymbol{u}^\alpha} G^\alpha \xrightarrow{\boldsymbol{v}^\alpha} B^\alpha$ is again an extension.

Suppose $\dim G = n$, $\dim B = m$ (hence $\dim A = n - m$). We say that a system $\sigma(\bar{\boldsymbol{x}}) = (\sigma_k(\bar{\boldsymbol{x}}))_{1 \leqq k \leqq n}$ of power series without constant terms in the $\bar{x}_i$ $(1 \leqq i \leqq m)$ is a *cross-section* for the extension $(G, \boldsymbol{u}, \boldsymbol{v})$ if $\boldsymbol{v}(\sigma(\bar{\boldsymbol{x}})) = \bar{\boldsymbol{x}}$; we have proved in Section 2 the existence of cross-sections for any extension. Then if we write (for a generic point $\boldsymbol{s}$ of G), $\boldsymbol{r}(\boldsymbol{s}) = \boldsymbol{s} \cdot (\sigma(\boldsymbol{v}(\boldsymbol{s})))^{-1}$, it is clear that $\boldsymbol{v}(\boldsymbol{r}(\boldsymbol{s})) = \bar{\boldsymbol{e}}$; hence, we see at once (taking, for instance, the subgroup $\boldsymbol{u}(A)$ of G in typical form) that we can write $\boldsymbol{r}(\boldsymbol{s}) = \boldsymbol{u}(\rho(\boldsymbol{s}))$, where $\rho(\boldsymbol{s})$ is a system $(\rho_j(\boldsymbol{s}))$ $(1 \leqq j \leqq n - m)$ of power series without constant terms. From the relation $\boldsymbol{s} = \boldsymbol{u}(\rho(\boldsymbol{s}))\sigma(\boldsymbol{v}(\boldsymbol{s}))$, it follows at once by considering the jacobians of the systems of power series on both sides, that the power series $t_j = \rho_j(\boldsymbol{s})$ $(1 \leqq j \leqq n - m)$ and $y_k = v_k(\boldsymbol{s})$ $(1 \leqq k \leqq m)$ define a change of variables in G; in other words, considering $\boldsymbol{t} = (t_j)$ as a generic point of A, $\boldsymbol{y} = (y_k)$ as a generic point of B, we can write $\boldsymbol{s} = \boldsymbol{u}(\boldsymbol{t})\sigma(\boldsymbol{y})$.

We will suppose from now on that, unless the contrary is explicitly

stated, A is *abelian*. We can then define on A a structure of *B-module*, by defining $\mathbf{y}\cdot\mathbf{t}'$ ($\mathbf{t}'$ second independent generic point of A) such that $\mathbf{u}(\mathbf{y}\cdot\mathbf{t}') = \sigma(\mathbf{y})\mathbf{u}(\mathbf{t}')(\sigma(\mathbf{y}))^{-1}$; the verification of axioms (3) and (4) is immediate, and (5) follows from the commutativity of A. On the other hand, we have, for a second independent generic point $\mathbf{y}'$ of B, $\mathbf{v}(\sigma(\mathbf{y})\sigma(\mathbf{y}')) = \mathbf{y}\mathbf{y}'$; hence $\sigma(\mathbf{y})\sigma(\mathbf{y}') = \mathbf{u}(\mathbf{a}(\mathbf{y},\mathbf{y}'))\sigma(\mathbf{y}\mathbf{y}')$, where $\mathbf{a}(\mathbf{y},\mathbf{y}') = \rho(\sigma(\mathbf{y})\sigma(\mathbf{y}'))$. Therefore writing A additively, we have

$$(14) \qquad \mathbf{u}(\mathbf{t})\sigma(\mathbf{y})\mathbf{u}(\mathbf{t}')\sigma(\mathbf{y}') = \mathbf{u}(\mathbf{t}+\mathbf{y}\cdot\mathbf{t}'+\mathbf{a}(\mathbf{y},\mathbf{y}'))\sigma(\mathbf{y}\mathbf{y}').$$

If we write the associativity condition, we find in the usual way that $\mathbf{a}(\mathbf{y},\mathbf{y}')$ is a 2-*cocycle* on B with values in A; conversely, given an arbitrary 2-cocycle $\mathbf{a}(\mathbf{y},\mathbf{y}')$, the formal Lie G group defined by the group law

$$\phi((\mathbf{t},\mathbf{y}),(\mathbf{t}',\mathbf{y}')) = (\mathbf{t}+\mathbf{y}\cdot\mathbf{t}'+\mathbf{a}(\mathbf{y},\mathbf{y}'),\mathbf{y}\mathbf{y}')$$

together with the homomorphisms $\mathbf{u}\colon \mathbf{t}\to(\mathbf{t},\mathbf{e})$ and $\mathbf{v}\colon(\mathbf{t},\mathbf{y})\to\mathbf{y}$ constitute an extension of B by A. Furthermore, if $\sigma'(\bar{\mathbf{x}})$ is a second cross-section, we can write $\sigma'(\mathbf{y}) = \mathbf{u}(\mathbf{c}(\mathbf{y}))\sigma(\mathbf{y})$, with $\mathbf{c}(\mathbf{y}) = \rho(\sigma'(\mathbf{y}))$, and the 2-cocycle corersponding to σ' is easily computed to be

$$\mathbf{a}'(\mathbf{y},\mathbf{y}') = \mathbf{a}(\mathbf{y},\mathbf{y}') + \mathbf{y}\cdot\mathbf{c}(\mathbf{y}') - \mathbf{c}(\mathbf{y}\mathbf{y}') + \mathbf{c}(\mathbf{y});$$

in other words, it differs from $\mathbf{a}(\mathbf{y},\mathbf{y}')$ by a 2-coboundary. We thus obtain, as in the classical theory, a one-to-one correspondence between classes of equivalent extensions of B by A, corresponding to the *same* structure of B-module on A, and the second cohomology group $H^2(B,A)$ corresponding to that structure. We can also interpret the extensions corresponding to the trivial cohomology class (so called *trivial extensions*) by the classical notion of *semi-direct product*: we need not here suppose A *commutative* (and we write it multiplicatively); if $\mathbf{y}$ is a generic point of B, $\mathbf{t}$ a generic point of A, we suppose given a system $\mathbf{t}^{\mathbf{y}}$ of power series without constant terms in the components of $\mathbf{t}$ and $\mathbf{y}$, such that $\mathbf{t}\to\mathbf{t}^{\mathbf{y}}$ is an automorphism of $A_{(L)}$ (for any perfect field L containing $K[[\mathbf{y}]]$), and $(\mathbf{t}^{\mathbf{y}})^{\mathbf{y}'} = \mathbf{t}^{\mathbf{y}'\mathbf{y}}$ for two independent points $\mathbf{y}$, $\mathbf{y}'$ of B; it is then easily verified that we define a group G by taking as group law

$$\phi((\mathbf{t},\mathbf{y}),(\mathbf{t}',\mathbf{y}')) = (\mathbf{t}\mathbf{t}'^{\mathbf{y}},\mathbf{y}\mathbf{y}').$$

We say that G is the *semi-direct product* of A and B, corresponding to the automorphism $\mathbf{t}\to\mathbf{t}^{\mathbf{y}}$; it is obvious that the homomorphisms $\mathbf{u}\colon\mathbf{t}\to(\mathbf{t},\mathbf{e})$ and $\mathbf{v}\colon(\mathbf{t},\mathbf{y})\to\mathbf{y}$ constitute with G an extension of B by A, and when A is abelian, it is clear that such an extension is trivial, and conversely, that

every trivial extension is a semi-direct product. Observe that $\boldsymbol{w}: \boldsymbol{y} \to (\boldsymbol{e}, \boldsymbol{y})$ is a monomorphism of B into G; we say also that G is the semi-direct product of its normal subgroup $\boldsymbol{u}(A)$ and its subgroup $\boldsymbol{w}(B)$; it is clear that $\boldsymbol{u}(A) \wedge \boldsymbol{w}(B) = \boldsymbol{e}$. It is important, however, to remark that when K has characteristic $p > 0$, and $\boldsymbol{u}$ and $\boldsymbol{w}$ are monomorphisms of groups A, B of dimensions $n - m, m$ into a group G of dimension n, such that $\boldsymbol{u}(A)$ is normal in G and $\boldsymbol{u}(A) \wedge \boldsymbol{w}(B) = \boldsymbol{e}$, it does not follow that G is isomorphic to a semi-direct product of A and B, but merely that it is *isogeneous* to such a product. Indeed, if we define $\boldsymbol{t}^{\boldsymbol{y}}$ such that $\boldsymbol{u}(\boldsymbol{t}^{\boldsymbol{y}}) = \boldsymbol{w}(\boldsymbol{y})\boldsymbol{u}(\boldsymbol{t})\boldsymbol{w}(\boldsymbol{y})^{-1}$, it is immediate that $\boldsymbol{t} \to \boldsymbol{t}^{\boldsymbol{y}}$ satisfies the preceding conditions, hence defines a semi-direct product G' of A and B; furthermore, $\boldsymbol{f}(\boldsymbol{t}, \boldsymbol{y}) = \boldsymbol{u}(\boldsymbol{t})\boldsymbol{w}(\boldsymbol{y})$ is a homomorphism of G' into G, and $\boldsymbol{u}(A)$ and $\boldsymbol{w}(B)$ are contained in G; hence as $G = \boldsymbol{u}(A) \vee \boldsymbol{w}(B)$ [9, Prop. 11, p. 354], $\boldsymbol{f}(G') = G$, and as G and G' have the same dimension, $\boldsymbol{f}$ is an isogeny. If we put $B_1 = G/\boldsymbol{u}(A)$, G is an extension of B_1 by A, and $\boldsymbol{v} \circ \boldsymbol{w}$ is an isogeny of B onto B_1, but, even when B and B_1 are isomorphic, G will not in general be a semi-direct product of $\boldsymbol{u}(A)$ and of a subgroup isomorphic to B_1: an example of that phenomenon is provided by taking $G = GL(n)$, $\boldsymbol{u}(A) = SL(n)$, and $\boldsymbol{w}(B)$ equal to the center Z of $GL(n)$, when n is a multiple of the characteristic p [9, p. 386]; if G were the semi-direct product of $SL(n)$ and of another group Z_1 (commuting with $SL(n)$), $Z \vee Z_1$ would be a two-dimensional subgroup of G contained in the center of that group, which is absurd.

Returning to the case in which A is abelian, we will therefore investigate under which conditions an extension $(G, \boldsymbol{u}, \boldsymbol{v})$ of B by A is isogeneous to a semi-direct product of A by a group isogeneous to B: we recall that for a formal Lie group G (resp. a homomorphism $\boldsymbol{u}$), $G^{(r)}$ (resp. $\boldsymbol{u}^{(r)}$) designates the group (resp. homomorphism) obtained by applying to the coefficients of the power series defining it the automorphism $\xi \to \xi^{p^r}$ of K (r a positive or negative integer); $\boldsymbol{p}^r$ is the isogeny of G onto $G^{(r)}$ such that $\boldsymbol{p}^r(\boldsymbol{x})$ is the system of power series $(x_i^{p^r})$ $(r \geqq 0)$.

PROPOSITION 2. *Suppose that the extension $(G, \boldsymbol{u}, \boldsymbol{v})$ of B by the abelian group A is defined by the 2-cocycle $\boldsymbol{f}(\boldsymbol{s}_1, \boldsymbol{s}_2)$ on B with values in A. In order that G be isogeneous to a semi-direct product of A by a group isogeneous to B, it is necessary and sufficient that there exist an integer $r \geqq 0$ and a 1-cochain $\boldsymbol{c}(\boldsymbol{s}_1) \in C^1(B, A^{(r)})$ such that*

$$\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\boldsymbol{s}_1), \boldsymbol{p}^r(\boldsymbol{s}_2)) = (\boldsymbol{p}^r(\boldsymbol{s}_1) \cdot \boldsymbol{c}(\boldsymbol{s}_2))^{(r)} - \boldsymbol{c}(\boldsymbol{s}_1\boldsymbol{s}_2) + \boldsymbol{c}(\boldsymbol{s}_1). \tag{15}$$

The "sums" on the right hand side are taken in $A^{(r)}$, and $(\boldsymbol{y}_1 \cdot \boldsymbol{t}_1)^{(r)}$

($\mathbf{y}_1$ generic point of $B^{(r)}$, $\boldsymbol{t}_1$ generic point of $A^{(r)}$) means, of course, the system of power series $\mathbf{y}_1 \cdot \boldsymbol{t}_1$ in which the coefficients have been raised to the power p^r.

To prove the necessity of the condition, suppose there is in G a subgroup B_0 such that $\boldsymbol{u}(A) \wedge B_0 = \boldsymbol{e}$ and $\boldsymbol{v}(B_0) = B$; $\boldsymbol{v}$ (restricted to B_0) is thus an isogeny of B_0 onto B. There is therefore an integer $r \geqq 0$ and an isogeny $\boldsymbol{g}$ of B onto $B_0^{(r)}$ (which is a subgroup of $G^{(r)}$) such that $\boldsymbol{v}^{(r)}(\boldsymbol{g}(\mathbf{y})) = \boldsymbol{p}^r(\mathbf{y})$ [9, proof of Prop. 2, p. 337]. We can thus write $\boldsymbol{g}(\mathbf{y}) = \boldsymbol{u}^{(r)}(\boldsymbol{c}(\mathbf{y}))\sigma^{(r)}(\boldsymbol{p}^r(\mathbf{y}))$, with $\boldsymbol{c}(y) = \rho^{(r)}(\boldsymbol{g}(\mathbf{y}))$; if we write that $\boldsymbol{g}(\mathbf{y}\mathbf{y}') = \boldsymbol{g}(\mathbf{y})\boldsymbol{g}(\mathbf{y}')$ and observe that $\sigma^{(r)}(\boldsymbol{p}^r(\mathbf{y}))\sigma^{(r)}(\boldsymbol{p}^r(\mathbf{y}')) = \boldsymbol{u}^{(r)}(\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\mathbf{y}), \boldsymbol{p}^r(\mathbf{y}')))\sigma^{(r)}(\boldsymbol{p}^r(\mathbf{y}\mathbf{y}'))$ we obtain condition (15).

Conversely, suppose that the condition is satisfied, and consider the semi-direct product G_1 of $A^{(r)}$ and $B^{(r)}$, relative to the $B^{(r)}$-module structure defined by $(\mathbf{y}_1 \cdot \boldsymbol{t}_1)^{(r)}$; it is then readily verified that the mapping

$$(\boldsymbol{t}, \mathbf{y}) \to (\boldsymbol{p}^r(\boldsymbol{t}) - \boldsymbol{c}(\mathbf{y}), \boldsymbol{p}^r(\mathbf{y})) \tag{16}$$

is an isogeny of G onto G_1, hence our conclusion.

When an extension $(G, \boldsymbol{u}, \boldsymbol{v})$ of B by A is such that $\boldsymbol{u}(A)$ is in the center of G, it is clear that B acts trivially on A, and conversely; we shall say that such extensions are *central*; such an extension is trivial if and only if G is the *direct product* of two subgroups isomorphic to A and B respectively. Therefore, Proposition 2 yields here a condition for a central extension to be a *quasi-direct product* of A and B: the relation (15) is here simplified, due to the fact that $(\mathbf{y}_1 \cdot \boldsymbol{t}_1)^{(r)} = \boldsymbol{t}_1$, and means simply that $\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\boldsymbol{s}_1), \boldsymbol{p}^r(\boldsymbol{s}_2))$ is a 2-*coboundary* in $C^2(B, A^{(r)})$. We will then say that the central extension is *quasi-trivial*. With that terminology:

COROLLARY 1. *Suppose that for every integer s (positive or negative), every central extension of $B^{(s)}$ by A is quasi-trivial; then if A' and B' are respectively isogeneous to A and B, every central extension of B' by A' is quasi-trivial.*

Let us first consider the case in which $B' = B^{(s)}$, $A' = A^{(t)}$, where s and t are arbitrary integers. If $\boldsymbol{f}$ is an arbitrary 2-cocycle on B' with values in A', $\boldsymbol{f}^{(-t)}$ is a 2-cocycle on $B^{(s-t)}$ with values in A, hence there is an integer $r \geqq 0$ such that

$$\boldsymbol{p}^r(\boldsymbol{f}^{(-t)}(\boldsymbol{s}_1, \boldsymbol{s}_2)) = d_2\boldsymbol{g}(\boldsymbol{s}_1, \boldsymbol{s}_2),$$

where $\boldsymbol{g} \in C^1(B^{(s-t)}, A^{(r)})$. It follows at once that

$$\boldsymbol{p}^r(\boldsymbol{f}(\boldsymbol{s}_1, \boldsymbol{s}_2)) = d_2\boldsymbol{g}^{(t)}(\boldsymbol{s}_1, \boldsymbol{s}_2),$$

where $\boldsymbol{g}^{(t)} \in C^1(B^{(s)}, A^{(r+t)}) = C^1(B', A'^{(r)})$.

Suppose next that $\boldsymbol{u}$ is an isogeny of B onto a group B', $\boldsymbol{v}$ an isogeny of A' onto A; if $\boldsymbol{f}$ is a 2-cocycle in $C^2(B', A')$, $\boldsymbol{v}(\boldsymbol{f}(\boldsymbol{u}(\boldsymbol{s}_1), \boldsymbol{u}(\boldsymbol{s}_2)))$ is a 2-cocycle in $C^2(B, A)$; hence there is an integer $r \geqq 0$ and a 1-cochain $\boldsymbol{g} \in C^1(B, A^{(r)})$ such that $\boldsymbol{p}^r(\boldsymbol{v}(\boldsymbol{f}(\boldsymbol{u}(\boldsymbol{s}_1), \boldsymbol{u}(\boldsymbol{s}_2)))) = d_2\boldsymbol{g}(\boldsymbol{s}_1, \boldsymbol{s}_2)$. But there are integers $s \geqq 0$, $t \geqq 0$, an isogeny $\boldsymbol{u}_1$ of $B'^{(-s)}$ onto B and an isogeny $\boldsymbol{v}_1$ of A onto $A'^{(t)}$ such that $\boldsymbol{u} \circ \boldsymbol{u}_1 = \boldsymbol{p}^s$, $\boldsymbol{v}_1 \circ \boldsymbol{v} = \boldsymbol{p}^t$; we have therefore

$$\boldsymbol{p}^{r+s+t}(\boldsymbol{f}^{(-s)}(\boldsymbol{s}_1, \boldsymbol{s}_2)) = d_2\boldsymbol{g}_1(\boldsymbol{s}_1, \boldsymbol{s}_2),$$

where $\boldsymbol{g}_1 = \boldsymbol{v}_1{}^{(r)} \circ \boldsymbol{g} \circ \boldsymbol{u}_1 \in C^1(B'^{(-s)}, A'^{(r+t)})$; hence, finally,

$$\boldsymbol{p}^{r+s+t}(\boldsymbol{f}(\boldsymbol{s}_1, \boldsymbol{s}_2)) = d_2\boldsymbol{g}_1{}^{(s)}(\boldsymbol{s}_1, \boldsymbol{s}_2),$$

and as $\boldsymbol{g}_1{}^{(s)} \in C^1(B', A'^{(r+s+t)})$, this, together with the treatment of the special case we considered first, ends the proof.

COROLLARY 2. *Suppose A is a quasi-direct product of abelian groups $A_1, \cdots, A_m$ and that for each integer s, every central extension of $B^{(s)}$ by any one of the A_i $(1 \leqq i \leqq m)$ is quasi-trivial. Then every extension of any $B^{(s)}$ by A is quasi-trivial.*

If A is the direct product of the A_i, the result is trivial, by decomposing a cocycle $\boldsymbol{f} \in C^2(B^{(s)}, A)$ into its components, which are cocycles belonging to the groups $C^2(B^{(s)}, A_i)$. The general case follows from that particular one and from Corollary 1.

PROPOSITION 3. *Let H be a normal subgroup in a formal Lie group G, and suppose that for every integer s the central extensions of $H^{(s)}$ and of $(G/H)^{(s)}$ by A are all quasi-trivial; suppose in addition that $H^1(M_{(N)}, A_{(N)}{}^{(r)}) = 0$ for any $r \geqq 0$ and any perfect extension N of K. Then any central extension of G by A is quasi-trivial.*

Suppose a central extension of G by A is defined by a 2-cocycle $\boldsymbol{f}(\boldsymbol{s}_1, \boldsymbol{s}_2)$; then, if ρ is the natural injection of H into G, $\boldsymbol{f}(\rho(\boldsymbol{t}_1), \rho(\boldsymbol{t}_2))$ ($\boldsymbol{t}_1, \boldsymbol{t}_2$ independent generic points in H) defines a central extension of H by A; by assumption, there is therefore an integer $r \geqq 0$ such that $\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\rho(\boldsymbol{t}_1)), \boldsymbol{p}^r(\rho(\boldsymbol{t}_2)))$ is a 2-coboundary in $C^2(H, A^{(r)})$. If we apply the exact sequence of Prop. 1 (with A replaced by $A^{(r)}$), we conclude that the cohomology class of the 2-cocycle $\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\boldsymbol{s}_1), \boldsymbol{p}^r(\boldsymbol{s}_2))$ is the image by λ^* of a cohomology class in $H^2(G/H, A^{(r)})$; i.e. there is a cochain $\boldsymbol{c}(\boldsymbol{s}_1) \in C^1(G, A^{(r)})$ and a cocycle $\boldsymbol{g} \in C^2(G/H, A^{(r)})$ such that

$$\boldsymbol{f}^{(r)}(\boldsymbol{p}^r(\boldsymbol{s}_1), \boldsymbol{p}^r(\boldsymbol{s}_2)) = \boldsymbol{g}(\bar{\boldsymbol{h}}(\boldsymbol{s}_1), \bar{\boldsymbol{h}}(\boldsymbol{s}_2)) + \boldsymbol{c}(\boldsymbol{s}_1) - \boldsymbol{c}(\boldsymbol{s}_1\boldsymbol{s}_2) + \boldsymbol{c}(\boldsymbol{s}_2). \tag{17}$$

On the other hand, it follows from the assumptions and from Cor. 1 to Prop. 2 that there is an integer $t \geqq 0$ such that $g^{(t)}(p^t(\tilde{s}_1), p^t(\tilde{s}_2))$ is equal to a 2-coboundary $c_1(\tilde{s}_1) - c_1(\tilde{s}_1\tilde{s}_2) + c_1(\tilde{s}_2)$ in $C^2(G/H, A^{(r+t)})$. If in each equation of th esystem (17), we raise both sides to the power p^t and use the preceding result, we finally get

$$f^{(r+t)}(p^{r+t}(s_1), p^{r+t}(s_2)) = c_2(s_1) - c_2(s_1 s_2) + c_2(s_2),$$

where $c_2(s) = c^{(t)}(p^t(s)) + c_1(\bar{h}(s))$ is a cochain in $C^1(G, A^{(r+t)})$; this ends the proof of Prop. 3.

6. The main theorems. We suppose from now on that K is a perfect field of characteristic $p > 0$; most of the time we will even assume that K is algebraically closed. All Lie groups are finite dimensional.

PROPOSITION 4. *Let T be a torus and A an abelian group over an algebraically closed field. If T operates trivially on A, then $H^2(T, A) = 0$.*

Suppose G is a central extension of T by A; then it follows from Lemma 3 in [9, p. 376] that G is abelian; we know, however, that the core of an abelian group is a direct factor, and that in a torus, any subgroup is a direct factor ([10, p. 128] or [5, p. 236, Th. 3 and p. 234, Prop. 6]); T is thus a direct factor in G, hence the conclusion.

We shall usually denote abelian Lie groups additively, and therefore write $x \to k \cdot x$ the "k-th power endomorphism" of such a group, for any integer k (which of course, for $k = p$, has to be sharply distinguished from the Frobenius homomorphism p of A onto $A^{(1)}$); it is obvious that when k is not divisible by p, that mapping is an automorphism of A; we shall say that an abelian Lie group A is *divisible* if $x \to p \cdot x$ is surjective, hence an *isogeny* of A onto itself; $x \to k \cdot x$ is then an isogeny for *any* integer k. We know [10, p. 122, Prop. 4] that any abelian Lie group is quasi-direct product of its largest divisible subgroup and its largest unipotent subgroup. We recall that I_∞ denotes the one-dimensional additive group.

PROPOSITION 5. *Any central extension of the group I_∞ by a divisible abelian group A is quasi-trivial.*

As all the groups $I_\infty^{(r)}$ are isomorphic, it is equivalent to prove that a central extension of I_∞ by any $A^{(r)}$ is quasi-trivial (Cor. 1 to Prop. 2). Let $f(s, t)$ be a 2-cocycle on I_∞ with values in A; we have thus

$$f(s + t, u) + f(s, t) = f(s, t + u) + f(t, u), \tag{18}$$

the sums on both sides being taken for the group law of A. Observe first that replacing t by 0 in (18) gives $\boldsymbol{f}(s,0)=\boldsymbol{f}(0,u)$, and as s and u are distinct indeterminates, this implies $\boldsymbol{f}(s,0)=\boldsymbol{f}(0,u)=0$. It also follows from (18) that $\boldsymbol{f}_1(s,t)=\boldsymbol{f}(s,t)+\boldsymbol{f}(t,s)$ is also a 2-cocycle, and as $\boldsymbol{f}_1(t,s)=\boldsymbol{f}_1(s,t)$, it defines an *abelian* extension of I_∞ by A. However, we know that such an extension is quasi-trivial [10, p. 122, Prop. 4], hence (Prop. 2) there is an integer $r\geqq 0$ and a 1-cochain $\boldsymbol{c}\in C^1(I_\infty, A^{(r)})$ such that

$$\boldsymbol{p}^r(\boldsymbol{f}(s,t)+\boldsymbol{f}(t,s))=\boldsymbol{c}(s)-\boldsymbol{c}(s+t)+\boldsymbol{c}(t). \tag{19}$$

If $p\neq 2$, $\boldsymbol{x}\to 2\cdot\boldsymbol{x}$ is an automorphism of $A^{(r)}$, hence there is a 1-cochain $\boldsymbol{c}_1\in C^1(I_\infty, A^{(r)})$ such that $\boldsymbol{c}(s)=2\cdot\boldsymbol{c}_1(s)$; if we denote by $\boldsymbol{f}_2(s,t)$ the 2-cocycle $\boldsymbol{p}^r(\boldsymbol{f}(s,t))-\boldsymbol{c}_1(s)+\boldsymbol{c}_1(s+t)-\boldsymbol{c}_1(t)$, (19) can be written $\boldsymbol{f}_2(s,t)+\boldsymbol{f}_2(t,s)=0$. For $p=2$, $\boldsymbol{x}\to 2\cdot\boldsymbol{x}$ is only an isogeny, and therefore we can only assert the existence of an integer $h\geqq 0$ and a 1-cochain $\boldsymbol{c}_1$ such that $\boldsymbol{p}^h(\boldsymbol{c}(s))=2\cdot\boldsymbol{c}_1(s)$; we will then take

$$\boldsymbol{f}_2(s,t)=\boldsymbol{p}^{r+h}(\boldsymbol{f}(s,t))-\boldsymbol{c}_1(s)+\boldsymbol{c}_1(s,t)-\boldsymbol{c}_1(t),$$

and we reach the same conclusion. Using Prop. 2, we see that the proof of Prop. 5 is reduced to that of the following statement: *a 2-cocycle* $f\in Z^2(I_\infty, A)$ *such that*

$$\boldsymbol{f}(s,t)+\boldsymbol{f}(t,s)=0 \tag{20}$$

is equal to 0.

We first remark that if in (18) we take $u=s$, then equation (20) yields $2\cdot\boldsymbol{f}(s+t,s)=2\cdot\boldsymbol{f}(t,s)$, and as A is divisible, this gives

$$\boldsymbol{f}(s+t,s)=\boldsymbol{f}(t,s), \tag{21}$$

hence also, by (20),

$$\boldsymbol{f}(s,s+t)=\boldsymbol{f}(s,t). \tag{22}$$

If we replace t in succession by $0, s, 2s, \cdots$, in (21), we get

$$\boldsymbol{f}(ks,s)=0 \text{ for every integer } k>0. \tag{23}$$

We claim that for any integer $k>0$

$$\boldsymbol{f}(ks,u)=k\cdot\boldsymbol{f}(s,u). \tag{24}$$

Use induction on k: replace s by ks and t by s in (18); by (23), we get $\boldsymbol{f}((k+1)s,u)=\boldsymbol{f}(ks,s+u)+\boldsymbol{f}(s,u)$; the inductive assumption and (22) yield $\boldsymbol{f}(ks,s+u)=k\cdot\boldsymbol{f}(s,s+u)=k\cdot\boldsymbol{f}(s,u)$, hence our assertion. Let now $k=p$ in (24); we have $p\cdot\boldsymbol{f}(s,u)=0$ and as A is divisible, this means $\boldsymbol{f}(s,u)=0$, q. e. d.

We can now state our main results.

THEOREM 1. *If G is a solvable group over an algebraically closed field, and D the largest divisible abelian group in the center of G, then D is a quasi-direct factor in G.*

Let us first assume that G is *nilpotent*, and let C be the center of G. Then G/C is a representable unipotent group, hence there is an increasing sequence of subgroups

$$H_0 = C \subset H_1 \subset H_2 \subset \cdots \subset H_{m-1} \subset H_m = G$$

such that H_i is normal in H_{i+1}, and H_{i+1}/H_i is isomorphic to the additive group I_∞ [9, p. 380, Th. 6, p. 376, Lemma 3 and p. 379, Prop. 37]. We already know the theorem holds when G is abelian [10, p. 122, Prop. 4]; hence, we can use induction on m: by Prop. 5 and the induction hypothesis, any central extension of I_∞ or of H_{m-1}/D by D is quasi-trivial. We shall then be able to apply Prop. 3, as soon as we have checked that there is no nontrivial homomorphism of a unipotent group into a divisible group: but for such a homomorphism $\boldsymbol{u}$, we have $p^k \cdot \boldsymbol{u}(\boldsymbol{x}) = \boldsymbol{u}(\boldsymbol{x}^{p^k}) = 0$ for sufficiently large k, hence $\boldsymbol{u} = 0$.

Consider now the general case. By applying Prop. 38 of [9, p. 382] to the quotient G/C of G by its center C, we see that there is a nilpotent normal subgroup H of G, containing C and such that G/H is a *torus*. We can again apply Prop. 3 to this case: for we have just proved that any central extension of H/D by D is quasi-trivial, and Prop. 4 shows that the same is true for any central extension of G/H by D; finally, as H/C and C/D are unipotent, so is H/D, hence every homomorphism of $(H/C)_{(N)}$ into $D_{(N)}$ (N perfect extension of K) is 0.

THEOREM 2. *If the center of a solvable Lie group G (over an algebraically closed field) does not contain any divisible abelian group, G is isogeneous to a semi-direct product of a torus and of its largest unipotent (normal) subgroup.*

Let C be the center of G; then G/C is isogeneous to a semi-direct product of its largest unipotent subgroup H_1 and of a torus T_1 [9, p. 382, Prop. 38]; if N is the inverse image of T_1 in G, Lemma 3 of [9, p. 376] shows that N is an abelian group, hence a direct product of C and of a torus T. On the other hand, as C is unipotent, it is clear that the inverse image H of H_1 is the largest unipotent subgroup of G. Finally, we have $T \vee H = G$ and $T \wedge H = \boldsymbol{e}$, since $T \wedge H$ is a unipotent subgroup of a torus.

COROLLARY. *Any solvable Lie group G (over an algebraically closed field) is isogeneous to a group G_1 which is the direct product of a divisible abelian group and of a semi-direct product of the largest unipotent subgroup of G_1 and of a torus.*

7. Two-dimensional Lie groups. We now know enough to give a complete description, up to isogeny, of all two-dimensional Lie groups over an algebraically closed field. If such a group G is abelian, its structure (up to isogeny) is described by Theorems 1 and 2 of [10], restricted to the case $n = 2$. On the other hand, it follows from Chevalley's theory [3] that G cannot be a simple non abelian group [9, p. 385, Th. 7] since such a group is at least 3-dimensional. If G is not an abelian group, it therefore contains a normal subgroup N of dimension 1; there are then two possible cases:

A) G is nilpotent, N is the center of G (the center of a nilpotent group cannot be reduced to $\boldsymbol{e}$);

B) G is solvable but not nilpotent; then the center of G is reduced to $\boldsymbol{e}$ (otherwise G would be nilpotent); hence, it follows from Theorem 2 that G is a semi-direct product of N and of a 1-dimensional torus T.

Case A. From Prop. 4 it follows that G/N cannot be a torus; on the other hand, G/N is a one-dimensional representable abelian group, hence can only be I_∞ [9, p. 379, Prop. 37]. From Prop. 5, it then follows that N cannot be divisible (otherwise G would be commutative), and therefore we also have $N = I_\infty$. The structure of G is then known if we can describe all central extensions of I_∞ by itself. This, however, has essentially been done by M. Lazard: he has determined all homogeneous polynomials $P(x, y)$ in two indeterminates, which satisfy the equation

$$P(x + y, z) + P(x, y) = P(x, y + z) + P(y, z)$$

[12, pp. 261-264], and any 2-cocycle f on I_∞ with values in I_∞ is clearly an infinite sum of such polynomials; of course, to get a noncommutative group G we have to take at least one of these polynomials such that $P(y, x) \neq P(x, y)$.

The nilpotent groups thus defined give rise to a number of interesting remarks. First, they obviously constitute a phenomenon which is special to characteristics $p > 0$, since it is well known that there are no nilpotent non abelian Lie algebras of dimension 2 over a field of characteristic 0. We next observe that N is the *unique* subgroup of G of dimension 1: any other such subgroup H would be commutative and commute with N, and moreover, we

would have necessarily $H \wedge N = \boldsymbol{e}$, hence $G = H \vee N$ [9, p. 354, Prop. 11], and therefore G would be a quasi-direct product of H and N (see Section 5), hence would be commutative. It follows that G is not the l. u. b. of all abelian subgroups of G, which disproves a natural conjecture made in [7, p. 443].

We will next prove the rather surprising result:

PROPOSITION 6. *There exists a unipotent non commutative group G of dimension 2 which is not representable.*

This will prove, in particular, that a central extension of a representable group by a representable group (in this case, both are I_∞) is not necessarily representable; the class of non representable Lie groups is thus much more extensive than might have been thought *a priori*. It will also do away with any hope of extending to formal Lie groups either Ado's theorem or Chevalley's theorem on the structure of general algebraic groups [13, p. 439, Th. 16] in a reasonable way: the natural conjecture would have been that a Lie group would be the quasi-direct product of a divisible abelian group and of a representable group, but our example will show that this is not even the case for nilpotent groups.

To construct our example, we suppose that the field K has an infinite degree of transcendancy over the prime field $\boldsymbol{F}_p$, and we denote by (e_{hk}) (for all pairs (h, k) of numbers such that $h > k \geqq 0$) a system of *algebraically independent* elements of K (over $\boldsymbol{F}_p$). We define the extension G by means of the 2-cocycle

$$f(x, x') = \sum_{h>k} e_{hk} x^{p^h} x'^{p^k},$$

the group law of G being therefore given by

$$\text{(25)} \qquad \begin{cases} x'' = \phi_1(x, x') = x + x' \\ y'' = \phi_2(x, y, x', y') = y + y' + \sum_{h>k} e_{hk} x^{p^h} x'^{p^k}. \end{cases}$$

The subgroup N is a typical subgroup defined by $x = 0$. We shall slightly simplify our general notations by writing (for $x_1 = x$, $x_2 = y$) D_h and X_h instead of D_{h1} and X_{h1}, $Y_h = D_h'$ instead of $X_{h2} = D_{h2}$. From (25) and the definition of X_h [4, p. 93], we deduce

$$\text{(26)} \qquad X_h = D_h + \Big(\sum_{m>h} e_{mh} x^{p^m}\Big) D_0' + S_h,$$

where S_h is a combination (with coefficients in $\boldsymbol{F}_p$) of terms each of which is a product of a certain number of terms $e_{ij} x^{p^i}$ with $j < h$, and of a certain number of D'_j and D_j with $j < h$. For $h = 0$, $S_h = 0$, hence

$$\text{(27)} \qquad [X_h, X_0] = e_{h0} Y_0.$$

If we want to compute similarly $[X_h, X_k]$ for $h > k$, we have (by definition) to form $D_h X_k - D_k X_h$ and to replace x by 0 in the result. We thus obtain

$$[X_h, X_k] = \bar{e}_{hk} Y_0 + \sum_{\alpha} \bar{e}_{hk\alpha} Z_\alpha, \tag{28}$$

where the Z_α have their usual meaning (elements of the structural basis, with of course $\alpha = (\alpha_1, \alpha_2)$), and the summation extends over the indices such that $|\alpha| \neq 1$ and $h(\alpha) < h$; in addition

$$\bar{e}_{hk} = e_{hk} - F_{hk}((e_{ij})), \tag{29}$$

where F_{hk} is a polynomial *with coefficients in* $\boldsymbol{F}_p$, in the e_{ij} such that either $i \leqq h$ and $j < k$, or $i < h$ (this is due to the fact that $D_k x^{p^i} = 0$ for $i > k$), and $\bar{e}_{hk,\alpha}$ is a polynomial, with coefficients in $\boldsymbol{F}_p$, in the e_{ij} such that either $i \leqq h$ and $j < k$, or $i < h$ (for the same reason). Similarly, if we express the X_α as linear combinations of the Z_λ, we see that if $h(\alpha) < h$, the coefficients are polynomials, with coefficients in $\boldsymbol{F}_p$, in the e_{ij} such that $i < h$. The group law of G will not in general be pseudo-canonical; but if we apply to it the "standard process" described in [9, p. 335] to transform it into a pseudo-canonical group law, it follows easily from our last remark and from the fact that in the free hyperalgebra the coefficients of the multiplication table are in $\boldsymbol{F}_p$, that after we have made the necessary change of variables, we still have (28) with similar properties for the coefficients $\bar{e}_{hk}$ and $\bar{e}_{hk\alpha}$ (although, of course, the polynomials F_{hk} will not be the same). We may therefore assume that the group law of G is pseudo-canonical.

We shall now assume that G is representable and show that this ultimately leads to a contradiction. Our assumption is therefore that there is a two-dimensional subgroup G' of a group $GL(n)$ (over K) which is isogeneous to G. Replacing, if necessary, G by some $G^{(r)}$, we can assume that there is an isogeny $\boldsymbol{u}$ of G onto G', and furthermore, that there is no trivial factor $\boldsymbol{p}$ in that isogeny. If we denote by $\mathfrak{G}$ (resp. $\mathfrak{G}'$, $\mathfrak{G}''$) the hyperalgebra of G (resp. $G', GL(n)$), by $\mathfrak{g}_h$ and $\hat{\mathfrak{s}}_h$ (resp. $\mathfrak{g}_h'$, $\mathfrak{g}_h''$ and $\hat{\mathfrak{s}}_h'$, $\hat{\mathfrak{s}}_h''$) the Lie algebra of invariant semi-derivations of height h and the associative subalgebra it generates in $\mathfrak{G}$ (resp. $\mathfrak{G}', \mathfrak{G}''$), our last assumption means that, for the derived mapping $\boldsymbol{u}'$: $\mathfrak{G} \to \mathfrak{G}'$, we have $\boldsymbol{u}'(\mathfrak{g}_0) \neq 0$. Let $\mathfrak{a}$ be the kernel of $\boldsymbol{u}'$, which is a two-sided ideal in $\mathfrak{G}$; if $\mathfrak{a} \neq 0$, we have $\mathfrak{a} \cap \mathfrak{g}_0 \neq 0$ (by the homomorphism theorem), and it follows from (27) that $\mathfrak{a} \cap \mathfrak{g}_0$ is the subspace consisting of the scalar multiples of Y_0. We next observe that, due to (27) and to the existence of the Frobenius homomorphism, the coefficient of Y_k on the right hand side of (28) is $e^{p^k}{}_{h-k,0} \neq 0$. It is then easy to see that $\mathfrak{a}$ is the ideal

generated by $Y_0, Y_1, \cdots, Y_{t-1}$ in G, if $\boldsymbol{u}$ is an isogeny of height t; this can be done either directly by using an argument similar to the proof of Theorem 1 in [9, p. 339-340], or by applying general characterizations of kernels of derived mappings of isogenies, which will be described in detail in a forthcoming publication of P. Cartier (see preliminary announcement in [2]); for that reason, we suppress the proof here. We can then write $\boldsymbol{u} = \boldsymbol{w} \circ \boldsymbol{v}$, where $\boldsymbol{v}$ is an isogeny of G onto a group $\bar{G}$, $\boldsymbol{w}$ an isomorphism of $\bar{G}$ onto G', and where $\bar{G}$ is the extension of I_∞ by itself corresponding to the 2-cocycle f^{p^t}.

We shall from now on replace G by $\bar{G}$; ignoring the effect of the automorphism $\xi \to \xi^{p^t}$ on the e_{hk}, we are thus reduced to proving that after replacing the e_{hj} for $j < t$ by 0 in our description of G, there can be no *isomorphism* $\boldsymbol{u}$ of G onto a subgroup G' of $GL(n)$. It is clear that if we write $X_h' = \boldsymbol{u}'(X_h)$, $Y_h' = \boldsymbol{u}'(Y_h)$, $Z_\alpha' = \boldsymbol{u}'(Z_\alpha)$, the Z_α' constitute a structural basis of $\mathfrak{G}'$, for which the group law of G' is pseudo-canonical: in other words, Z_α' is equal to a noncommutative polynomial in the X_k' and Y_k' such that $k \leqq h(\alpha)$, *with coefficients in* $\boldsymbol{F}_p$. Using this fact, we will now prove the following statement:

(*) *There is an increasing sequence* (L_h) *of fields over* $\boldsymbol{F}_p$, *such that* L_h *is generated over* $\boldsymbol{F}_p$ *by* $2n^2(h+1)$ *elements, and that the* Z_α' *with* $h(\alpha) \leqq h$ *are linear combinations of the basis of* $\mathfrak{g}_h''$ *with coefficients in* L_h.

We use induction on h: for $h = 0$, X_0' and Y_0' are linear combinations of the basis of $\mathfrak{g}_0''$; we take for L_0 the field generated over $\boldsymbol{F}_p$ by the $2n^2$ coefficients of these linear combinations. We assume throughout that we have taken the group law in $GL(n)$ in its natural form [9, p. 364] so that the multiplication table of the corresponding basis of $\mathfrak{G}''$ has its coefficients in $\boldsymbol{F}_p$. We denote by Δ the "structural mapping" of $\mathfrak{G}''$ into $\mathfrak{G}'' \otimes \mathfrak{G}''$, which induces the structural mapping of $\mathfrak{G}'$ into $\mathfrak{G}' \otimes \mathfrak{G}'$. The element X_h' satisfies the relation

$$\Delta(X_h') - 1 \otimes X_h' - X_h' \otimes 1 = \sum Z_\alpha' \otimes Z_\beta' \tag{30}$$

the summation being extended to all pairs such that $|\alpha| \neq 1$, $|\beta| \neq 1$, $\alpha + \beta = p^h \epsilon_1$. If we express X_h' as a linear combination of the basis of $\mathfrak{g}_h''$, relation (30) is equivalent to a system of (non homogeneous) linear equations, where the unknowns are the coefficients of that linear combination, and the coefficients and right hand terms are *in the field* L_{h-1}, due to our inductive assumption. We know that there is an element X_h' in $\mathfrak{G}'$ which satisfies (30); this means that the equivalent system of linear equations has a solution consisting of *elements of* K; but from the preceding remark, it follows that

it has also a solution consisting of *elements of* L_{h-1}. Let X_h'' be the element of $\mathfrak{G}''$ which is determined by that second solution; we shall have in general $X_h'' \neq X_h'$, but it follows from (30) that the difference $X_h'' - X_h'$ is a *derivation*, in other words, it belongs to $\mathfrak{g}_0''$. Similarly, there is an element Y_h'' in $\mathfrak{G}''$ which is a linear combination of the basis of $\mathfrak{g}_h''$ with coefficients in L_{h-1}, and such that $Y_h'' - Y_h'$ is in $\mathfrak{g}_0''$; if we express these two elements of $\mathfrak{g}_0''$ as linear combinations of the basis of that Lie algebra, and denote by L_h the field obtained by adjoining to L_{h-1} the coefficients of these combinations ($2n^2$ in all), we have shown that the basis of $\mathfrak{g}_h'$ can be expressed as linear combinations of the basis of $\mathfrak{g}_h''$ with coefficients in L_h. It follows that the coefficients of the multiplication table for the basis of $\mathfrak{g}_h'$ belong to L_h. The other elements Z_α' of the basis of $\mathfrak{s}_h'$ are therefore (by the remark preceding statement (*)) linear combinations of the basis of $\mathfrak{s}_h''$ with coefficients in L_h, and our induction is thus complete.

We are now ready to derive our final contradiction. For any h, it follows from (*) and (28) that the coefficients $\bar{e}_{ij}$ $(j < i \leqq h)$ belong to L_h. However, there are $(h-t)(h-t+1)/2$ such elements which are algebraically independent over $\boldsymbol{F}_p$; hence the inequality

$$(h-t)(h-t+1)/2 \leqq 2n^2(h+1)$$

which certainly cannot be verified when h is taken large enough; q. e. d.

If we do not assume that the e_{hk} are algebraically independent, we can, of course, obtain representable groups, and even algebraic groups: the simplest of these is the group of 3×3 matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & x^p & 1 \end{pmatrix}.$$

More generally, if in the preceding matrix, we replace x^p by

$$g(x) = e_1 x^p + e_2 x^{p^2} + \cdots + e_h x^{p^h} + \cdots,$$

where the e_h are arbitrary elements of K, we define a monomorphism into $GL(3)$ of the group G corresponding to the 2-cocycle

$$f(x, x') = \sum_{h \geqq 1} e_h x^{p^h} x'. \tag{31}$$

We can, however, prove

PROPOSITION 7. *If in* (31) *the* e_h *are algebraically independent over* $\boldsymbol{F}_p$, *then* G *is not an algebraic group* (or, more precisely, G cannot be *isogeneous* to a formal Lie group of the type G'^*, where G' is an algebraic group).

In other words, if we consider in *any* $GL(n)$ a formal subgroup G_1 isogeneous to G, we shall always have $\dim \mathcal{A}(G_1) > \dim G_1$ for its algebraic hull $\mathcal{A}(G_1)$.

We may suppose that K is algebraically closed without restricting the generality. We first investigate the structure of an algebraic group G' which has a center C' isomorphic to the additive group K, and which is such that G'/C' is also isomorphic to K: indeed, if G is isogenous to G'^*, G' will necessarily be of this type, for the center C of G has then to be isogeneous to C'^*, and G/C to G'^*/C'^* [9, Props. 18 and 21], and there is only one algebraic group formally isogeneous to I_x, namely the additive group K. Now, a result of Rosenlicht [13, p. 426, Th. 10] proves the existence of a (rational) cross-section $\sigma: G'/C' \to G'$; this cross-section will in general only be defined in an open set U of K (for the Zariski topology), but we shall show that there is then another cross section which is *everywhere defined* in K. Indeed, let u be a biregular isomorphism of the additive group K onto the center C' (which, like G', we write multiplicatively). If π is the natural homomorphism of G' onto G'/C' (which we identify with K), let $\rho(s) = s \cdot (\sigma(\pi(s)))^{-1}$; this is a rational mapping of G' into C', defined in $\pi^{-1}(U)$. The complement of U in K consists of a *finite* number of points x_i $(1 \leqq i \leqq m)$; let $x_0 \in U$ be such that all the points $x_0 + x_i$ $(1 \leqq i \leqq m)$ are also in U, and consider the rational function (from K to K)

$$\phi(x) = u^{-1}(\rho(\sigma(x)\sigma(x_0)));$$

at each of the points x_i $(1 \leqq i \leqq m)$ this function may have a pole; there is, at any rate, a rational function $\psi(x)$ which has poles *at most* at the x_i $(1 \leqq i \leqq m)$, and is such that $\phi(x) - \psi(x)$ is *regular* at all these points. Consider then the cross-section

$$\sigma'(x) = \sigma(x)(u(\psi(x)))^{-1};$$

it is certainly regular outside the x_i $(1 \leqq i \leqq m)$; we show that it is also regular at these points. Indeed, we have

$$\sigma'(x)\sigma(x_0) = \sigma(x)\sigma(x_0)(u(\psi(x)))^{-1} = \psi(x + x_0)u(\phi(x) - \psi(x)),$$

and as the right hand side is regular at each of the x_i, so is $\sigma'(x)$.

We may thus suppose that σ is regular on K; then ρ is also defined everywhere on G, and

$$a(x, x') = u^{-1}(\rho(\sigma(x)\sigma(x')))$$

is a 2-cocycle which is a rational function *defined everywhere* on $K \times K$, hence a *polynomial* in x and x'. We conclude that there is a biregular isomorphism of G' onto a group G_1 defined by the group law

$$(32)\qquad \begin{cases} \phi_1^{(1)}(x, x') = x + x' \\ \phi_2^{(1)}(x, y, x', y') = y + y' + f_1(x, x'), \end{cases}$$

where f_1 is a polynomial 2-cocycle.

We now proceed to show that there is no isogeny of G_1 onto G. By the same argument as in the proof of Prop. 6, one is immediately reduced to proving that there is no *isomorphism* $\boldsymbol{u} = (u_1(x, y), u_2(x, y))$ of G_1 onto G. Such an isomorphism must of course map the center C_1 of G_1 onto the center C of G; hence, the relation $x = 0$ must imply $u_1(0, y) = 0$; this means that in the power series $u_1(x, y)$, every monomial contains x. However, we must have

$$(33)\qquad u_1(x + x', y + y' + f_1(x, x')) = u_1(x, y) + u_1(x', y'),$$

and if $u_1(x, y)$ actually contained y, by considering the monomials of smallest degree in y, and among them, the one with smallest degree in x (the latter being $\neq 0$, as seen above), it is clear that there would be in the left hand side of (33) terms containing both x' and y, which cannot be matched by similar terms on the right hand side. Hence u_1 must be an additive power series in x, i. e.

$$u_1(x) = a_0 x + a_1 x^p + \cdots + a_k x^{p^k} + \cdots \qquad (a_0 \neq 0).$$

A similar argument, applied to the relation

$$(34)\qquad u_2(x + x', y + y' + f_1(x, x')) = u_2(x, y) + u_2(x', y') + f(u_1(x), u_1(x'))$$

shows that there are no monomials in $u_2(x, y)$ which can contain both x and y, i. e. $u_2(x, y) = v(x) + w(y)$. Replacing x and x' by 0 in (34) shows that w is an additive power series, i. e.

$$w(y) = b_0 y + b_1 y^p + \cdots + b_k y^{p^k} + \cdots \qquad (b_0 \neq 0),$$

and then (34) boils down to

$$(35)\qquad g(u_1(x)) \cdot u_1(x') = v(x + x') - v(x) - v(x') + w(f_1(x, x')).$$

We claim that it is impossible that *both* $g \circ u_1$ and u_1 be polynomials: indeed, this would imply that the relations

$$e_k b_0^{p^k} + e_{k-1} b_1^{p^{k-1}} + \cdots + e_1 b_{k-1} = 0$$

hold from a certain k on, with only finitely many of the b_k being $\neq 0$; but this would obviously imply that the e_k are not algebraically independent over $\boldsymbol{F}_p$. However, if $g \circ u_1$ has infinitely many terms, there are on the left hand side of (35) terms of the form $x^{p^k} x'$ with arbitrarily high values of k.

But in $w(f_1(x,x'))$, the terms of the form $x^h x'$ have *bounded* exponents h since f_1 is a polynomial, and if there were in $v(x+x')-v(x)-v(x')$ a term in $x^{p^k}x'$, there would be a term in xx'^{p^k} (with same coefficient) which cannot be cancelled by terms of $w(f_1(x,x'))$ for the same reason as above, and is not matched by any term on the left hand side. If on the contrary, $g \circ u_1$ is a polynomial, then u_1 has infinitely many terms $\neq 0$; hence there are on the left hand side terms in $x^p x'^{p^k}$ with arbitrarily high k, and no terms in $x^{p^k}x'^p$ as soon as k is large enough; an argument quite similar to the preceding one shows that (35) is again impossible in that case, and the proof of Prop. 7 is complete.

8. *Case B.* In sharp contrast with the rather pathological features of case A, we shall prove

PROPOSITION 8. *Every solvable non nilpotent group G of dimension 2 is isomorphic to one of the (algebraic) groups of matrices*

$$\begin{pmatrix} 1+s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & (1+s)^{p^h} \end{pmatrix}$$

and all these groups are isogeneous.

As G is a semi-direct product of a normal subgroup isomorphic to I_x and of a subgroup isomorphic to I_0, we have to determine all the possible structures of I_0-module on I_x. As $x \to s \cdot x$ is an automorphism of I_x (over a field containing $K[[s]]$), we can write $s \cdot x = \sum_{k=0}^{\infty} a_k(s) x^{p^k}$. It is readily verified that the group of automorphisms of I_x can be considered as an infinite dimensional formal Lie group A, which is recursive in the sense of [6, p. 55], and can be neatly described, in a self-explanatory way, as the group of infinite triangular matrices

$$(36) \qquad \begin{pmatrix} 1+x_1 & x_2 & x_3 & \cdots & x_n & \cdots \\ 0 & (1+x_1)^p & x_2{}^p & \cdots & x_{n-1}{}^p & \cdots \\ 0 & 0 & (1+x_1)^{p^2} & \cdots & x_{n-2}{}^{p^2} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & (1+x_1)^{p^{n-1}} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

The system of power series $(a_k(s))$ constitutes a homomorphism $s \to M(s)$ of I_0 into that group A; equivalently, this means that for every n, the first

n series $a_k(s)$ constitute a homomorphism $s\to M_n(s)$ of I_0 into the group A_n obtained by taking only the first n rows and columns in the infinite matrix (36). In particular, $A_1=I_0$, and therefore we must have $1+a_0(s)=(1+s)^\zeta$, where ζ is an arbitrary p-adic integer [5, p. 241, Th. 5]. We claim now that for any k, $a_k(s)$ is a linear combination of the power series $(1+s)^{p^h\zeta}-(1+s)^\zeta$ for $0\leqq h\leqq k$. To prove this, we use induction on k and observe that the group A_n, which has dimension n, is a semi-direct product of a nilpotent group and of a one-dimensional torus, namely the subgroup of diagonal matrices $(1+x_1, (1+x_1)^p, \cdots, (1+x_1)^{p^{n-1}})$. We may assume $\zeta\neq 0$, otherwise it would be easily checked that all the a_k of index $k\geqq 1$ would be 0 (there is no homomorphism $\neq 0$ of I_0 into a unipotent group); from A. Borel's conjugation theorem [1, p. 56, Th. 12.2] it follows that there is a unipotent triangular matrix P_k of order k such that $P_kM_k(s)P_k^{-1}$ is the diagonal matrix $((1+s)^\zeta, \cdots, (1+s)^{p^{k-1}\zeta})$. If we denote by P the infinite triangular matrix $\begin{pmatrix} P_k & 0 \\ 0 & I \end{pmatrix}$, we see that by replacing the homomorphism $s\to M(s)$ by $s\to PM(s)P^{-1}$, we may suppose that $a_1(s)=\cdots=a_{k-1}(s)=0$. The relation $M(s+t+st)=M(s)M(t)$ then yields, in particular,

$$\begin{aligned} a_k(s+t+st) &= (1+s)^\zeta a_k(t)+a_k(s)\,(1+t)^{p^k\zeta} \\ &= (1+t)^\zeta a_k(s)+a_k(t)\,(1+s)^{p^k\zeta}, \end{aligned}$$

and as t and s are independent indeterminates, this is only possible if $a_k(s)=c_k((1+s)^{p^k\zeta}-(1+s)^\zeta)$. Returning to our original $M(s)$, this proves our assertion.

Now let $\zeta=p^h\epsilon$, where ϵ is a p-adic unit. In the group G, we may change variables by taking new variables s_1, x_1 such that $1+s_1=(1+s)^\epsilon$ and $x_1=x$. The new group law corresponds to a structure of I_0-module on I_∞ in which $\zeta=p^h$; we may thus assume from now on that this condition is satisfied. It is then clear that we have

$$s\cdot x=(1+s)^q c_0(x)+(1+s)^{pq}c_1(x^p)+\cdots+(1+s)^{p^nq}c_n(x^{p^n})+\cdots,$$

where $c_0(x)=x+c_{01}x^p+\cdots$ and, in general,

$$c_n(x)=c_{n0}x+c_{n1}x^p+\cdots+c_{nm}x^{p^m}+\cdots,$$

and we have written for simplicity $q=p^h$. We then change variables again, taking this time $s_1=s$ and $x_1=c_0(x)$; this amounts (again dropping the indices 1) to supposing that $c_0(x)=x$; but if we then again write relation (5), we see easily that the $c_n(x)$ of index $\geqq 1$ must be 0: supposing in fact

that r is the first index such that $c_r(x) \neq 0$, we see that in the identity, the term $(1+s)^q(1+t)^{qp^r}c_r(x^{p^r})$ is not matched by any other term, hence the assumption $c_r \neq 0$ leads to a contradiction. This ends the proof of Prop. 8, and we thus see that for characteristic $p \neq 0$, the structure of solvable non nilpotent groups of dimension 2 is pretty much the same as for characteristic 0, if we disregard the isogenies. I do not know if this extends to dimensions $\geqq 3$.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956), pp. 20-82.

[2] P. Cartier, "Calcul différentiel sur les variétés algébriques en caractéristique non nulle," *Comptes Rendus Hebdomadaires des Séances de l'Academie des Sciences, Paris*, vol 245 (1957), pp. 1109-1111.

[3] C. Chevalley, "Classification des groupes de Lie algébriques," *Séminaire École Normale Supérieure*, 1956-57.

[4] J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 87-118.

[5] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, (II)," *American Journal of Mathematics*, vol. 77 (1955), pp. 218-244.

[6] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, (III)," *Mathematische Zeitschrift*, vol. 63 (1955), pp. 53-75.

[7] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV)," *American Journal of Mathematics*, vol. 77 (1955), pp. 429-452.

[8] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (V)," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 207-239.

[9] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI)," *American Journal of Mathematics*, vol. 79 (1957), pp. 331-388.

[10] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (VII)," *Mathematische Annalen*, vol. 134 (1957), pp. 114-133.

[11] G. Hochschild-J-P. Serre, "Cohomology of group extensions," *Transactions of the American Mathematical Society*, vol. 74 (1953), pp. 110-134.

[12] M. Lazard, "Sur les groupes de Lie formels à un paramètre," *Bulletin de la Société Mathématique de France*, vol. 83 (1955), pp. 251-274.

[13] M. Rosenlicht, "Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp. 401-443.

ON SOME INVARIANTS OF CYCLOTOMIC FIELDS.*

By KENKICHI IWASAWA.**

Dedicated to Professor E. Artin on His Sixtieth Birthday

1. Let p be an odd prime. For each $n \geqq 0$, we denote by ζ_n a primitive p^n-th root of unity and by K_n the cyclotomic field obtained by adjoining ζ_{n+1} to the rational field Q: $K_n = Q(\zeta_{n+1})$. It is proved in [4] that if p^{e_n} is the highest power of p dividing the class number of K_n, then the exponent e_n is given, for all sufficiently large n, by a formula

$$e_n = \lambda n + \mu p^n + \nu, \qquad n \geqq n_0, \tag{1}$$

where λ, μ and ν are integers independent of n. The numbers λ and μ seem to have deep significance for the arithmetic of the fields K_n. In general, if the invariant $\mu = \mu(K/F)$ of a so-called Γ-extension K over a finite algebraic number field F is 0, then the Galois group of the maximal unramified abelian p-extension over K is, up to a finite subgroup, isomorphic with the direct sum of λ copies of the additive group of p-adic integers, where $\lambda = \lambda(K/F)$ denotes another invariant of K/F.[1] So, if $\mu = 0$, we have an analogue, for number fields, of a similar result for algebraic function fields of one variable over algebraically closed fields of constants. For this and other reasons, it seems interesting to know whether $\mu > 0$ or $\mu = 0$ for a given Γ-extension K/F, and we shall find in the present paper necessary and sufficient conditions for $\mu > 0$ when the Γ-extension is obtained from the cyclotomic fields K_n defined above, namely, when μ is given as the second coefficient in the above formula (1).

2. Let K be the union of all K_n, $n \geqq 0$. K is an abelian extension of Q and, for any element σ of the Galois group $G(K/Q)$, there exists a unique p-adic unit ξ such that

$$\sigma(\zeta_n) = \zeta_n^{\xi},$$

for every $n \geqq 0$. The mapping $\sigma \to \xi$ then defines a topological isomorphism

* Received February 6, 1958.

** Guggenheim Fellow. The present research was also supported in part by a National Science Foundation grant.

[1] Cf. [4], § 5, § 7.

of $G(K/Q)$ with the multiplicative group U of p-adic units and we denote the Galois automorphism σ corresponding to ξ by σ_ξ. Under this isomorphism, the subgroup $G(K/K_n)$ of $G(K/Q)$ corresponds to the subgroup U_n of all ξ in U satisfying $\xi \equiv 1 \bmod. p^{n+1}$. On the other hand, the group U is the direct product of U_0 and a cyclic group V of order $p-1$, the group of all roots of unity in the p-adic number field Q_p. The corresuonding subgroup Δ of $G(K/Q)$ is then canonically isomorphic with the Galois group $G(K_0/Q)$, and $G(K/Q)$ is the direct product of Δ and $\Gamma = G(K/K_0) \cong U_0$.

Now, suppose that Δ acts continuously on a compact p-primary abelian group N. Since N is p-primary, the element u^α is defined as usual for any u in N and for any p-adic integer α. For each i, $1 \leqq i \leqq p-1$, let $N^{(i)}$ be the set of all u in N such that

$$\sigma_\eta(u) = u^{\eta^i},$$

for every η in V, i.e., for every σ_η in Δ. It is then easy to see that each $N^{(i)}$ is a closed subgroup of N and N is the direct product of these $N^{(i)}$:

$$N = N^{(1)} \times \cdots \times N^{(p-1)}.$$

Let L be the maximal unramified abelian p-extension over K. Then L is a Galois extension of Q, and $G(K/Q) = \Gamma \times \Delta$ acts on the abelian normal subgroup $G(L/K)$ of $G(L/Q)$ in a natural way. For each $n \geqq 0$, let L_n denote the maximal unramified abelian p-extension of K_n. L is then the union of all L_n and, p^{e_n} being the degree of the extension L_n/K_n, the formula (1) was proved in [4] by studying the structure of the Γ-group $G(L/K)$.

We now apply the above decomposition to the Δ-group $G(L/K)$ and obtain

$$G(L/K) = G(L/K)^{(1)} \times \cdots \times G(L/K)^{(p-1)}.$$

We denote by $L^{(i)}$ $(1 \leqq i \leqq p-1)$ the subfield of L containing K such that

$$G(L/L^{(i)}) = \prod_{j \neq i} G(L/K)^{(j)}, \qquad G(L^{(i)}/K) \cong G(L/K)^{(i)}.$$

Since Δ may be considered as acting on the Galois group $G(L_n/K_n)$ in a natural way, $G(L_n/K_n)$ can be also decomposed with respect to Δ and we obtain subfields $L_n^{(i)}$ $(1 \leqq i \leqq p-1)$ of L_n containing K_n, defined similarly as the above $L^{(i)}$. Clearly, the action of Γ on $G(L/K)$ commutes with the action of Δ on $G(L/K)$. Hence $G(L^{(i)}/K)$ $(1 \leqq i \leqq p-1)$ are again Γ-groups like $G(L/K)$. Using the fact that $L^{(i)}$ is the union of all $L_n^{(i)}$, $n \geqq 0$, it can be proved in the same way as in [4] that if $p^{e_n^{(i)}}$ is the degree of the extension $L_n^{(i)}/K_n$, then the exponent $e_n^{(i)}$ is given, for all sufficiently large n, by

$$e_n^{(i)} = \lambda^{(i)} n + \mu^{(i)} p^n + \nu^{(i)}, \qquad (1 \leqq i \leqq p-1), \tag{2}$$

where $\lambda^{(i)}$, $\mu^{(i)}$ and $\nu^{(i)}$ are again integers independent of n. Since $e_n = \sum_{i=1}^{p-1} e_n^{(i)}$, we obtain from (1) and (2) that

$$\lambda = \sum_{i=1}^{p-1} \lambda^{(i)}, \qquad \mu = \sum_{i=1}^{p-1} \mu^{(i)}, \qquad \nu = \sum_{i=1}^{p-1} \nu^{(i)}.$$

Let e_n^+ be the sum of $e_n^{(i)}$ with even i and let e_n^- be the sum of $e_n^{(i)}$ with odd i. Similarly, we define λ^+, λ^-, μ^+, μ^- and ν^+, ν^- as the sums of $\lambda^{(i)}$, $\mu^{(i)}$ and $\nu^{(i)}$ with even or odd indices respectively. Then,

$$e_n = e_n^+ + e_n^-, \quad \lambda = \lambda^+ + \lambda^-, \quad \mu = \mu^+ + \mu^-, \quad \nu = \nu^+ + \nu^-.$$

Furthermore, if L_n^+ denotes the composite of all $L_n^{(i)}$ with even i and L_n^- the composite of all $L_n^{(i)}$ with odd i, then $p^{e_n^+}$ and $p^{e_n^-}$ are the degrees of the extensions of L_n^+/K_n and L_n^-/K_n respectively, and they are also equal to the highest powers of p dividing, respectiveliy, the second and the first factors of the class number of K_n.[2]

LEMMA 1. *$\mu = 0$ if and only if $\mu^- = 0$.*

Proof. As the proof of (1) shows, $\mu = 0$ ($\mu^- = 0$) if and only if the rank of $G(L_n/K_n)$ ($G(L_n^-/K_n)$) is bounded for every $n \geqq 0$. However, it is a classical result that

$$\operatorname{rank} G(L_n^+/K_n) \leqq \operatorname{rank} G(L_n^-/K_n) \leqq \operatorname{rank} G(L_n/K_n) \leqq 2 \operatorname{rank} G(L_n^-/K_n).$$[3]

The lemma then follows immediately.

Remark. By a similar method as in [7], we can obtain a more precise result:

$$\operatorname{rank} G(L_n^{(i)}/K_n) \leqq \operatorname{rank} G(L_n^{(j)}/K_n), \qquad n \geqq 0,$$

where i is even, j is odd and $i + j \equiv 1 \bmod p - 1$.

3. Assume, now, that $\mu > 0$. Then, by the above lemma, $\mu^- > 0$ and, hence, $\mu^{(i)} > 0$ for some odd index i. We fix such an index $i = a$. The Galois group $G(L^{(a)}/K)$ is then a so-called regular strictly Γ-finite compact Γ-group with the invariant $\mu^{(a)} > 0$, and it follows that, for each $n \geqq 0$, $G(L_n^{(a)}/K_n)$ contains a subgroup which is, as a $G(K_n/K_0)$-group, isomorphic with the additive group of the group ring of $G(K_n/K_0)$ over the prime field of characteristic p.[4] Let P_n be the p-Sylow group of the absolute ideal class

[2] More generally, if F is a subfield of K_0 with $[K_0 : F] = d$ and K' is the Γ-extension defined naturally over F, then the invariants of K'/F are given by the sums of $\lambda^{(i)}$ and $\mu^{(i)}$ with the indices i divisible by d.

[3] Cf. [7].

[4] Cf. [4], § 5 and a forthcoming paper of the author.

group of K_n and let $P_n^{(a)}$ be the a-th direct factor of the Δ-decomposition of P_n. By class field theory, $G(L_n^{(a)}/K_n)$ is then canonically isomorphic with $P_n^{(a)}$. Hence, by the above, there exists an ideal class C_0 of order p in $P_n^{(a)}$ such that $\sigma_\eta(C_0) = C_0^{\eta^a}$ for every η in V and that the classes $\sigma_\xi(C_0)$ are independent when ξ runs over p-adic units in $U_0 \bmod. U_n$.

Now, for any p-adic integer α, let $s_n(\alpha)$ $(n \geqq 0)$ denote the uniquely determined rational integer such that

$$\alpha \equiv s_n(\alpha) \bmod. p^{n+1}, \qquad 0 \leqq s_n(\alpha) < p^{n+1}.$$

For any ideal class C in P_n and for any ξ in U, we have then

$$\prod_\alpha \sigma_\alpha(C)^{d(\alpha)} = 1, \tag{3}$$

where the product is taken over all α in $U \bmod. U_n$ and the exponent $d(\alpha)$ is given by

$$d(\alpha) = p^{-(n+1)}(s_n(\xi\alpha^{-1}) - \xi s_n(\alpha^{-1})).$$

This is a special case of a general identity which holds for the ideal classes and their conjugates of a cyclotomic field. For the field K_0, it is given in [3], § 109 and the general case can be deduced easily from the result in [5].

Applying (3) to the above ideal class C_0, we obtain

$$\sum_{\eta \in V} (s_n(\xi\eta^{-1}) - \xi s_n(\eta^{-1}))\eta^a \equiv 0 \bmod. p^{n+2}, \qquad \xi \in U,$$

or

$$\sum_\eta s_n(\xi\eta^{-1})\eta^a \equiv \xi \sum_\eta s_n(\eta^{-1})\eta^a \bmod. p^{n+2}, \qquad \xi \in U. \tag{4}$$

First, we put $\xi = 1 + p^{n+1}$ in the above. Since $s_n(\xi\eta^{-1}) = s_n(\eta^{-1})$, we have

$$\sum_\eta s_n(\eta^{-1})\eta^a \equiv (1 + p^{n+1}) \sum_\eta s_n(\eta^{-1})\eta^a \bmod. p^{n+2},$$

and, hence, also

$$\sum_\eta s_n(\eta^{-1})\eta^a \equiv 0 \bmod. p.$$

As $s_n(\eta^{-1}) \equiv \eta^{-1} \bmod. p$, it follows that $a \neq 1$.

Next, we take ξ from V, in (4). Then the left hand side is equal to $\xi^a \sum_\eta s_n(\eta^{-1})\eta^a$ and, as $a \neq 1$, $1 \leqq a \leqq p-1$, it follows that

$$\sum_\eta s_n(\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+2}.$$

Hence, by (4),

$$\sum_\eta s_n(\xi\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+2}, \qquad \eta \in V, \tag{5}$$

for any ξ in U. We have thus proved that the assumption $\mu > 0$ implies (5)

for some odd index $a \neq 1$ and for every $n \geqq 0$. Notice that (5) does not hold for $a = 1$ (and $n = 0$).

To prove the converse of the above, we use the classical formula for the first factor of the class number of K_n.[5] Let Ω_p be the algebraic closure of Q_p and χ a character of U with values in Ω_p^* such that $\chi(U_n) = 1$. Put

$$S_n(\chi) = p^{-(n+1)} \sum_{\xi} s_n(\xi)\chi(\xi),$$

where ξ runs over p-adic units in U mod. U_n. We notice that $S_n(\chi)$ is an element of Ω_p and that if $\chi(U_m) = 1$ for $m \leqq n$, then $S_n(\chi) = S_m(\chi)$. Now, the classical formula tells us that the highest power of p dividing the first factor of the class number of K_n is equal to the highest power of p dividing, in Ω_p, the product

$$p^{n+1} \prod_{\chi} S_n(\chi), \tag{6}$$

where χ runs over all characters of U such that $\chi(U_n) = 1$ and $\chi(-1) = -1$.

Suppose that (5) holds for an odd index a. Clearly, there exist p^n characters χ of U such that $\chi(U_n) = 1$ and that $\chi(\eta) = \eta^{-a}$ for every η in V. Since a is odd, these characters satisfy $\chi(-1) = -1$ and the corresponding $S_n(\chi)$ appear in the product (6). It is also clear that (5) implies

$$S_n(\chi) \equiv 0 \text{ mod. } p,$$

for any such character χ. On the other hand, it is known that the product of p^{n+1} and other factors $S_n(\chi')$ in (6) is an integer of Ω_p. Hence the product (6) is divisible by p^{p^n} and we obtain that

$$e_n^- \geqq p^n.$$

Since $e_n^- = \lambda^- n + \mu^- p^n + \nu^-$, it follows that if (5) holds for every $n \geqq 0$, then $\mu^- > 0$ and, consequently, $\mu > 0$. Thus the following result is proved:

I. *The second coefficient μ in the formula* (1) *is positive if and only if there exists an odd integer a, $1 \leqq a \leqq p-1$, such that* (5) *holds for any p-adic unit ξ and for any $n \geqq 0$.*

For any p-adic integer α, let

$$\alpha = \sum_{k=0}^{\infty} t_k(\alpha) p^k, \qquad 0 \leqq t_k(\alpha) < p,$$

be the canonical p-adic expansion of α. Then,

$$s_n(\alpha) = \sum_{k=0}^{n} t_k(\alpha) p^k, \qquad s_{n+1}(\alpha) = s_n(\alpha) + t_{n+1}(\alpha) p^{n+1}.$$

[5] For the following, cf. [2], § 5, § 33.

Since $a \not\equiv 1$ and

$$\sum_{\eta} s_{n+1}(\xi\eta^{-1})\eta^a \equiv \sum_{\eta} \xi\eta^{a-1} \equiv 0 \bmod. p^{n+2},$$

the condition (5) is equivalent with the following:

$$\sum_{\eta} t_{n+1}(\xi\eta^{-1})\eta^a \equiv 0 \bmod. p, \qquad n \geqq 0.$$

Notice that it holds trivially

$$\sum_{\eta} t_0(\xi\eta^{-1})\eta^a \equiv 0 \bmod. p.$$

4. We now consider that the roots of unity ζ_n are all contained in Ω_p and asume that $\zeta_{n+1} = \zeta_n$. $n \geqq 0$. We have then

$$p^{n+1}/(\zeta_{n+1} - 1) = \sum_{i=0}^{p^{n+1}-1} i\zeta_{n+1}{}^i = \sum_{\alpha} s_n(\alpha)\zeta_{n+1}{}^{\alpha},$$

where α runs over all p-adic integers mod. p^{n+1}. For any η in V, it follows that

$$p^{n+1}/(\zeta_{n+1}{}^{\eta} - 1) = \sum_{\alpha} s_n(\alpha)\zeta_{n+1}{}^{\alpha\eta} = \sum_{\alpha} s_n(\alpha\eta^{-1})\zeta_{n+1}{}^{\alpha}.$$

If $n \geqq 1$, we have similarly

$$p^{n+1}/(\zeta_n{}^{\eta} - 1) = p\sum_{\beta} s_{n-1}(\beta\eta^{-1})\zeta_n{}^{\beta} = \sum_{\beta} s_n(p\beta\eta^{-1})\zeta_{n+1}{}^{p\beta},$$

where β runs over all p-adic integers mod. p^n. Therefore,

$$p^{n+1}(1/(\zeta_{n+1}{}^{\eta} - 1) - 1/(\zeta_n{}^{\eta} - 1)) = \sum_{\xi} s_n(\xi\eta^{-1})\zeta_{n+1}{}^{\xi},$$

where ξ runs over all p-adic units in U mod. U_n.

Now, for each $n \geqq 0$ and i, $1 \leqq i \leqq p-1$, put

$$T_n{}^{(i)} = \sum_{\eta \in V} \eta^i/(\zeta_{n+1}{}^{\eta} - 1).$$

Then the above computation shows that, for any $n \geqq 0$,

$$(7) \qquad p^{n+1}(T_n{}^{(i)} - T_{n-1}{}^{(i)}) = \sum_{\xi} \left(\sum_{\eta} s_n(\xi\eta^{-1})\eta^i\right)\zeta_{n+1}{}^{\xi}, \qquad \xi \text{ in } U \bmod. U_n.$$

For convenience, we put here

$$T_{-1}{}^{(i)} = 0, \qquad 1 \leqq i \leqq p-1.$$

Suppose that there exists an odd index a, $1 \leqq a \leqq p-1$, such that (5) holds for any p-adic unit ξ and for any $n \geqq 0$. Then, it follows from (7) that

$$T_n{}^{(a)} \equiv T_{n-1}{}^{(a)} \bmod. p, \qquad n \geqq 0,$$

and, as $T_{-1}^{(a)} = 0$, we also have that

$$T_n^{(a)} \equiv 0 \bmod. p, \qquad n \geqq 0. \tag{8}$$

To prove the converse, we first notice the following

LEMMA 2. *Suppose that*

$$\sum_{\xi} a_\xi \zeta_{n+1}{}^{\xi} \equiv 0 \bmod. p^s, \qquad \xi \text{ in } U \bmod. U_n,$$

with a_ξ *in* Q_p. *Then, for any* ω *in* U,

$$\sum_{\xi}{}' a_\xi \equiv 0 \bmod. p^s,$$

where ξ *runs over all p-adic units* mod. U_n *such that* $\xi \equiv \omega \bmod. U_{n-1}$.[6]

The proof is elementary and, hence, is omitted here.

Now, assume that (8) holds for an odd index a and for any $n \geqq 0$. It then follows from (7) that

$$\sum_{\xi} \Big(\sum_{\eta} s_n(\xi\eta^{-1})\eta^a\Big)\zeta_{n+1}{}^{\xi} \equiv 0 \bmod. p^{n+2}.$$

By Lemma 2, we have, for any ω in U, that

$$\sum_{\xi}{}' \sum_{\eta} s_n(\xi\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+2}, \qquad \xi \equiv \omega \bmod. U_{n-1}. \tag{9}$$

Suppose that $n \geqq 1$ and put

$$\xi \equiv \omega + jp^n \bmod. p^{n+1}, \qquad 0 \leqq j < p.$$

Then,

$$s_n(\xi\eta^{-1}) = s_{n-1}(\omega\eta^{-1}) + kp^n, \qquad 0 \leqq k < p, \tag{10}$$

where k *is* determined by

$$k \equiv t_n(\omega\eta^{-1}) + j\eta^{-1} \bmod. p.$$

If ξ runs over p-adic units mod. U_n such that $\xi \equiv \omega \bmod. U_{n-1}$, k runs over all integers from 0 to $p-1$, and we obtain from (9) and (10) that

$$p \sum_{\eta} s_{n-1}(\omega\eta^{-1})\eta^a + p^n \sum_{k} \sum_{\eta} k\eta^a \equiv 0 \bmod. p^{n+2}.$$

Since $a \not\equiv 0 \bmod. p-1$, $\sum_{\eta} \eta^a = 0$ and it follows that

$$\sum_{\eta} s_{n-1}(\omega\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+1}, \qquad n \geqq 1.$$

Thus, we see that (5) holds for any ξ in U and for any $n \geqq 0$, and the following result is proved:

[6] For $n = 0$, we understand $U_{-1} = 1$.

II. *The second coefficient μ in the formula* (1) *is positive if and only if there exists an odd integer a, $1 \leqq a \leqq p-1$, such that*

$$\sum_{\eta} \eta^a/(1-\zeta_{n+1}{}^{\eta}) \equiv 0 \bmod. p, \qquad \eta \in V, \tag{11}$$

for every $n \geqq 0$.

5. Let O_p be the ring of p-adic integers and $Q_p((x))$ the field of all power series in x with coefficients in Q_p. We denote by R the subring of those power series in $Q_p((x))$ which have coefficients in O_p, and by R_0 the subring of integral power series in R. Let $\alpha \neq 0$ be a non-unit integer in Ω_p. Then, for any $\phi = \phi(x)$ in R, the element $\phi(\alpha)$ in Ω_p is well defined and $\phi \to \phi(\alpha)$ gives a ring homomorphism of R into Ω_p. In particular, if $\alpha = 1-\zeta_{n+1}$, it induces a homomorphism of R_0 onto the ring of all integers in $Q_p(\zeta_{n+1})$.

Let a be an odd integer and η any element of V. The power series for $(1-x)^{\eta}$, defined in the usual way, is then contained in R_0 and we have

$$\eta^a/(1-(1-x)^{\eta}) = \eta^{a-1}/x + \phi_{\eta}(x),$$

with a power series ϕ_{η} in R_0. Putting $x = 1-\zeta_{n+1}$ in the above, it follows that

$$\sum_{\eta} \eta^a/(1-\zeta_{n+1}{}^{\eta}) = (1-\zeta_{n+1})^{-1} \cdot \sum_{\eta} \eta^{a-1} + \sum_{\eta} \phi_{\eta}(1-\zeta_{n+1}),$$

where $\phi_{\eta}(1-\zeta_{n+1})$ are integers in $Q_p(\zeta_{n+1})$.

Now, suppose that (11) holds for every $n \geqq 0$. The above equality then shows that $a \neq 1$ and that

$$\sum_{\eta} \phi_{\eta}(1-\zeta_{n+1}) \equiv 0 \bmod. p.$$

Using the fact that the elements $(1-\zeta_{n+1})^i$, $0 \leqq i < (p-1)p^n$, form a basis of the ring of integers in $Q_p(\zeta_{n+1})$ over O_p, it follows that

$$\sum_{\eta} \phi_{\eta}(x) \equiv 0 \bmod. pR_0 + x^{(p-1)p^n} R_0.$$

Since n is an arbitrary non-negative integer, we have then

$$\sum_{\eta} \phi_{\eta}(x) \equiv 0 \bmod. p,$$

and, consequently,

$$\sum_{\eta} \eta^a/(1-(1-x)^{\eta}) \equiv 0 \bmod. p.^{7}$$

Clearly, we can reverse the above argument and see that the above congruence conversely implies (11) for every $n \geqq 0$. Therefore:

---

[7] mod. p means mod. pR_0 or mod. pR.

III. *The second coefficient* μ *in the formula* (1) *is positive if and only if there exists an odd integer* a, $1 \leqq a \leqq p-1$, *such that*

$$\sum_{\eta} \eta^a/(1-(1-x)^{\eta}) \equiv 0 \bmod. p, \qquad \eta \in V. \tag{12}$$

Remark. III can be proved also by a different method using the classical formula for the second factor of the class number of K_n.

Now, if an element $\pi = \pi(x)$ of R_0 is of the form

$$\pi(x) = c_1 x + c_2 x^2 + \cdots, \qquad c_1 \in U,$$

there exists an automorphism of R over O_p which maps x to $\pi(x)$. Therefore, (12) is equivalent with

$$\sum_{\eta} \eta^a/(1-(1-\pi(x))^{\eta}) \equiv 0 \bmod. p, \tag{13}$$

for any such π. Choosing a suitable power series for œ, we can further transform the condition (12).

Consider the formal power series $L(x)$ and $E(x)$ defined by

$$L(x) = \sum_{i=0}^{\infty} x^{p^i}/p^i, \qquad E(x) = e^{-L(x)}.^{8}$$

As power series in $Q_p((x))$, they have the properties:

$$\eta L(x) = L(\eta x), \qquad E(x)^{\eta} = E(\eta x),$$

for any η in V. It is also known that $E(x)$ can be written in the form

$$E(x) = \prod_{m} (1-x^m)^{\mu(m)/m},$$

where $\mu(m)$ is the Mobius function and m runs over all positive rational integers prime to p. Hence $E(x)$ is contained in R_0 and it holds that

$$E(x) \equiv 1 - x \bmod. x^2 R_0.$$

Putting $\pi(x) = 1 - E(x)$ in (13), we then obtain

$$\sum_{\eta} \eta^a/(1-E(\eta x)) \equiv 0 \bmod. p.$$

Now, let $\sum_k a_k x^k$ be the power series for $(1-E(x))^{-1}$ and put

$$\psi_i(x) = \sum_{k \equiv i (p-1)} a_k x^k, \qquad 1 \leqq i \leqq p-1.$$

Then the left hand side of the above congruence is nothing but $(p-1)\psi_{p-a-1}(x)$ and we have immediately the following result:

---

[8] Cf. [1].

IV. *Let $\psi_i(x)$ be defined as above. Then the second coefficient μ in the formula* (1) *is positive if and only if there exists an odd integer a, $1 \leqq a \leqq p-1$, such that*

$$\psi_a(x) \equiv 0 \bmod. p.$$

The advantage of IV lies in that we can explicitly calculate $\psi_i(x)$, $1 \leqq i \leqq p-1$, by using the classical power series:

$$1/(1-e^{-z}) = 1/z + \tfrac{1}{2} - \sum_{n=1}^{\infty} (-1)^n B_n z^{2n-1}/(2n)!,$$

where B_n $(n \geqq 1)$ are the Bernoulli numbers. Put $z = L(x)$ in the above and notice that the exponents of x which appear in the power series $L(x)$ are always congruent with $1 \bmod. p-1$. We then obtain immediately that

$$\begin{aligned}
&\psi_{p-1}(x) = \tfrac{1}{2}, \\
&\psi_i(x) = 0, && 2 \mid i, i \neq p-1, \\
&\psi_{p-2}(x) = L(x)^{-1} - \textstyle\sum^{(p-2)} (-1)^n B_n L(x)^{2n-1}/(2n)!, \\
&\psi_i(x) = -\textstyle\sum^{(i)} (-1)^n B_n L(x)^{2n-1}/(2n)!, && 2 \nmid i, i \neq p-2,
\end{aligned}$$

where $\sum^{(i)}$ means the summation over all $n \geqq 1$ such that $2n-1 \equiv i \bmod. p-1$.

Now, it is clear from the above that $\psi_{p-2}(x) \not\equiv 0 \bmod. p$.[9] For an odd $a \neq p-2$, we can then calculate the coefficients of $x^{a+k(p-1)}$, $k \geqq 0$, in $\psi_a(x)$ from the last equality and, putting them to be congruent to $0 \bmod. p$, we obtain a sequence of congruence relations on the Bernoulli numbers which altogether form an equivalent condition with $\psi_a(x) \equiv 0 \bmod. p$. For instance, we obtain from the first two coefficients the following congruences:

$$\begin{aligned}
&B'(\tfrac{1}{2}(a+1)) \equiv 0 \bmod. p, \\
&B'(\tfrac{1}{2}(a+1)) \equiv B'(\tfrac{1}{2}(a+1) + \tfrac{1}{2}(p-1)) \bmod. p^2,
\end{aligned}$$

where $B'(n)$ is defined by

$$B'(n) = (-1)^n B_n/n, \quad . \qquad n \geqq 1.$$

The first congruence in the above shows that if $\mu > 0$, i.e., if $\psi_a(x) \equiv 0 \bmod. p$ for some odd a, p must be an irregular prime. But this can be otherwise proved easily without making use of the above result.

For the irregular primes $p = 37, 59, 67$, we can determine the index a for which the first congruence is satisfied, and then see that the second

[9] This corresponds to the fact that (5), (11) and (12) do not hold for $a = 1$.

congruence does not hold for such an a.[10] Hence, we have $\mu = 0$ for these prime numbers. However, in these cases, it is also known that the order of $G(L_1/K_1)$ is p^2 and, by the structural theorem on Γ-groups,[11] we can prove more precisely that $G(L/K)$ is isomorphic with Γ and that $\lambda = 1$, $\mu = 0$ and $\nu = 0$.

Remark. Using the fact that the coefficients of the power series for $(1-E(x))^{-1}$ are always p-adic integers, we can obtain, by a similar argument as above, various congruence relations for the Bernoulli numbers mod. p^n.

THE INSTITUTE FOR ADVANCED STUDY
AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] E. Artin and H. Hasse, "Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln," *Abhandlungen aus dem Mathematischen Seminar der Hamburg Universität*, vol. 6 (1928), pp. 146-162.

[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin, 1952.

[3] D. Hilbert, "Die Theorie der algebraischen Zahlkörper," *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 4 (1897), pp. 175-546.

[4] K. Iwasawa, "On Γ-extensions of algebraic number fields," to appear shortly in *Bulletin of the American Mathematical Society*.

[5] R. E. MacKenzie, "Class group relations in cyclotomic fields," *American Journal of Mathematics*, vol. 74 (1952), pp. 759-763.

[6] F. Pollaczek, "Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln," *Mathematische Zeitschrift*, vol. 21 (1924), pp. 1-38.

[7] T. Takagi, "Zur Theorie der Kreiskörpers," *Journal für die reine und angewandte Mathematik*, vol. 157 (1927), pp. 230-238.

[10] Cf. [6].

[11] Cf. [4], § 5.

ON A THEOREM OF TORELLI.* [1]

By T. MATSUSAKA.

Let Γ be a complete non-singular surve, J^g be its Jacobian variety and α be the canonical mapping of Γ into J. Let θ be a *canonical divisor on J with respect to* Γ, which is determined uniquely up to translations. By means of $\mathfrak{L}(m\theta)$, we can embed J into a projective space, i.e. $m\theta$ is *linearly effective*, whenever m is sufficiently large (cf. Weil [8]). Therefore, the set $\mathfrak{X}$ of positive divisors X on J, such that $s\theta \equiv tX \bmod G_n(J)$ for two positive integers s and t, defines a *structure of polarization* on J (cf. Weil [9], Matsusaka [4]). When J is polarized this way, we call it the *canonically polarized Jacobian variety with respect to* Γ. The purpose of this paper is to show that when two canonically polarized Jacobian varieties are isomorphic, then two curves are isomorphic. First this theorem was proved by Torelli (Torelli [5]) in the classical case and another proof was given recently by Andreotti also in the classical case (Andreotti [1]). Quite recently, A. Weil showed that Andreotti's idea can be generalized to the abstract case (Weil [10]). The present author will show that Torelli's idea can also be generalized to the abstract case.

Let C be another complete non-singular curve, J'^g be the Jacobian variety of C and α' be the canonical mapping of C into J'. Let θ' be a canonical divisor on J' with respect to C and $\mathfrak{X}'$ be the set of positive J'-divisors which defines the canonical polarization on J' with respect to C. Let us assume that there is an isomorphism β between two thus polarized Jacobian varieties. Then β must be an isomorphism of the underlying Jacobian varieties satisfying $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Therefore, we make the following identification hereafter: we identify α' with $\beta^{-1} \cdot \alpha'$ and J' with J. Then J is the Jacobian variety of Γ, and at the same time, the Jacobian variety of C; moreover, canonical divisors θ and θ' on J with respect to Γ and C satisfy $\theta \equiv \theta' \bmod G_n(J)$. When that is so, there is a point d on J such that $\theta' = \theta_d$ by Weil [7], Cor. 2, Th. 32. We fix a common field k of definition for $\Gamma, C, J, \alpha, \alpha', \theta, d$ and regard k as a *basic field. All fields we shall consider shall be assumed to contain k.*

* Received February 14, 1958.

[1] We shall follow the same terminology and conventions as in [4], [6] and [7].

We shall denote by W^r (resp. V^r) the locus of $\sum_1^r \alpha(x_i)$ (resp. $\sum_1^r \alpha'(y_i)$) over k, where $(x_1, \cdots, x_r)$ (resp. $(y_1, \cdots, y_r)$) is a set of r independent generic points of Γ (resp. C) over k. We assume that $W^{g-1} = \theta$, $V^{g-1} = \theta'$. We have $W^1 = \alpha(\Gamma)$, $V^1 = \alpha'(C)$; we shall write W for W^{g-2} and V for V^{g-2}. Let $\mathfrak{k}$ and $\mathfrak{k}'$ be rational canonical divisors of Γ and C respectively over k. Denoting by δ the identity automorphism of J, $-\delta + S(\alpha(\mathfrak{k}))$ leaves θ invariant, and also $-\delta + S(\alpha'(\mathfrak{k}'))$ leaves θ' invariant (cf. Weil [7], Prop. 19). Let U be any subvariety of J, then we shall denote by U^- the transform of U by $-\delta$. We shall denote by W^* (resp. V^*) the transform of W (resp. V) by $-\delta + S(\alpha(\mathfrak{k}))$ (resp. $-\delta + S(\alpha'(\mathfrak{k}'))$).

Let now A be an arbitrary Abelian variety and X, Y be two subvarieties of A. Let x and y be independent generic points of X and Y over a common field of definition K for X and Y. We shall denote by $X \oplus Y$ the locus of $x+y$ over K. This definition can be extended to a finite set of positive A-cycles by linearity.

1. LEMMA 1. *$W_{\alpha(x)}$ and $W^*_{-\alpha(x)}$ are subvarieties of θ for all x on Γ. When x is a generic point of Γ over k, then $W_{\alpha(x)}$ and $W^*_{-\alpha(x)}$ contain generic points of θ over k.*

Proof. $W_{\alpha(x)}$ is a subvariety of θ by the definitions of W and θ. Since θ is invariant by the automorphism $-\delta + S(\alpha(\mathfrak{k}))$ of the underlying variety of J, $W^*_{-\alpha(x)}$ is also a subvariety of θ. By the same reason as above, when $W_{\alpha(x)}$ contains a generic point of θ over k, then so does $W^*_{-\alpha(x)}$. Assume now that x is a generic point of Γ over k, and let $w = \sum_1^{g-2} \alpha(x_i)$ be a generic point of W over $k(x)$. Then $(x, x_1, \cdots, x_{g-2})$ is a set of independent generic points of Γ over k; hence $w + \alpha(x)$ is a generic point of θ over k. Our lemma is thereby proved.

LEMMA 2. *Let U be a subvariety of co-dimension 1 on θ and w be a point of W. Then $U \cap \alpha(\Gamma)_w \neq \phi$.*

Proof. Let K be a field of definition for U and u be a generic point of U over K. Then u can be written uniquely as $u = \sum_1^{g-1} \alpha(x_i)$, where the x_i are points on Γ, otherwise $U \oplus \alpha(\Gamma)$ is a subvariety of W^* (cf. Weil [7], Prop. 16), which is a contradiction since $\dim U \oplus \alpha(\Gamma) = g-1$. We can find a set of $g-2$ independent generic points of Γ over K, say $(x_1, \cdots, x_{g-2})$, from the set $(x_1, \cdots, x_{g-1})$. Put $w = \sum_1^{g-2} \alpha(x_i)$, then w is a generic point of W over K. $\alpha(\Gamma)_w$ is a subvariety of θ and contains u. Hence $\alpha(\Gamma)_w \cap U$ is not empty, and from this our lemma follows immediately.

LEMMA 3. i) *Let D be a curve on J; then $D_t \cap V^*$ is not empty if and only if t is a point of $V^* \oplus D^-$.* ii) *$\alpha(\Gamma)_t$ is a subvariety of $\theta'_{\alpha'(y)}$ with y on C if and only if t is a point of $W_{d+\alpha'(y)}$.* iii) $W_d \oplus \alpha'(C) = V^* \oplus \alpha(\Gamma)^-$.

Proof. Let $S(\alpha'(\mathfrak{k}')) - v$ be a point in $D_t \cap V^*$. There is a point x on D such that $t = S(\alpha'(\mathfrak{k}')) - v - x$, which shows that t is on $V^* \oplus D^-$. Conversely, if t is on $V^* \oplus D^-$, then D_t and V^* have clearly a point in common. i) is thereby proved.

Assume that $\alpha(\Gamma)_t$ is on $\theta'_{\alpha'(y)}$. Since $\theta' = \theta_d$, $\alpha(\Gamma)_{t-d-\alpha'(y)}$ is contained in θ. By Weil [7], Th. 20, $\alpha(\Gamma)_{t-d-\alpha'(y)}$ is contained in θ if and only if $\alpha'(y) + d - t$ is on W^-. Therefore it is contained in θ if and only if t is a point of $W_{d+\alpha'(y)}$. ii) is thereby proved.

By our Lemma 1, $V^*_{-\alpha'(y)}$ is a subvariety of $\theta' = \theta_d$ for all y on C; hence $V^*_{-\alpha'(y)-d}$ is a subvariety of θ for all y on C. If we show that V^* and $\alpha(\Gamma)_{w+d+\alpha'(y)}$ have non-empty intersection for all w on W and y on C, then $W_d \oplus \alpha'(C)$ is contained in $V^* \oplus \alpha(\Gamma)^-$; and when that is so, we have $W_d \oplus \alpha'(C) = V^* \oplus \alpha(\Gamma)^-$ since both have the same dimension. Since $\alpha(\Gamma)_{w+d+\alpha'(y)} \cap V^* \neq \phi$ and $\alpha(\Gamma)_w \cap V^*_{-d-\alpha'(y)} \neq \phi$ imply each other, iii) follows from our Lemma 2.

2. Let X^r be the subvariety of $W^r \times \Gamma$ defined over k, defined by the following conditions: Let w be a generic point of W^r over k, then $X(w) = \mathfrak{m}$ is a positive Γ-divisor, $\deg(\mathfrak{m}) = r$ and $S(\alpha(\mathfrak{m})) = w$ (cf. Weil [7], Th. 18 and Weil [6], Chap. VII, Th. 12). We are going to study some properties of X when $r = g$ and $r = g - 1$. Whenever D is a curve on W^r such that $X^r \cdot (D \times \Gamma)$ is defined, we write

$$(D \times \Gamma) \cdot X = T + \mathfrak{a} \times \Gamma + D \times \mathfrak{b},$$

where every component of T has the projection D on D and Γ on Γ. We have obviously $\deg(\mathfrak{b}) \leqq r$ from the definition of X.

LEMMA 4. *Let t be a point on J. Then $(t \times \Gamma) \cdot X^g$ is defined on $J \times \Gamma$ if and only if t is not a point of W^*. Let D be a curve on J. Then $(D_t \times \Gamma) \cdot X^g$ is defined on $J \times \Gamma$ if and only if D_t is not a subvariety of W^*.*

Proof. If t is not a point of W^*, then denoting by v a generic point of J over k, $X(v)$ has the uniquely determined specialization $\mathfrak{m}$ over $v \to t$ ref. k, since $S(\alpha(\mathfrak{m}))$ must be t (cf. Weil [7], Prop. 16). Hence $(t \times \Gamma) \cdot X$ is defined. Conversely, if t is a point of W^*, then for any point x on Γ, there is a positive Γ-divisor $\mathfrak{m}$ of degree g such that $\mathfrak{m} - x > 0$ and that $S(\alpha(\mathfrak{m})) = t$. When that is so, it is easy to see that $(X(v), v) \to (\mathfrak{m}, t)$ ref. k and this implies that $(t \times \Gamma) \cdot X$ is not defined.

Assume that D_t is not contained in W^*; then the preceding result shows that $D_t \times \Gamma$ cannot be contained in X. Hence $(D_t \times \Gamma) \cdot X$ is defined since X is a divisor on $J \times \Gamma$. On the other hand, if D_t is a subvariety of W^*, $u \times \Gamma$ is contained in X for any point u on D_t. Therefore $(D_t \times \Gamma) \cdot X$ is not defined, and our Lemma is thereby proved.

LEMMA 5. *Let D be a curve on J and u be a point on J such that $(D_u \times \Gamma) \cdot X^g$ is defined.* (i) *A point t on D_u is a component of $\mathfrak{a}$ if and only if it is a component of $D_u \cap W^*$. When $D = \alpha'(C)$, then $\mathfrak{a} \neq 0$ if and only if $\mathfrak{b} \neq 0$.* (ii) *When u is a generic point of J over a field K over which D is defined, then $\mathfrak{a} = 0$.* (iii) *Assume that $D = \alpha'(C)$ and let x be a generic point of Γ over $K(u)$. If we put $\mathfrak{n} = {}^tT(x) + \mathfrak{a}$, we have*

$$S(\alpha(\mathfrak{n})) = \alpha(x) + (g-1)u + S(\alpha'(\mathfrak{k}')) - d.$$

Proof. Let t be a component of $\mathfrak{a}$. Then $(t \times \Gamma) \cdot X$ is not defined and t is a point of W^* by Lemma 4. Conversely, if t is a point in $D_u \cap W^*$, then $t \times \Gamma$ is contained in X by Lemma 4, which shows that t is a component of $\mathfrak{a}$. When $D = \alpha'(C)$, $D_u \cap W^* \neq \phi$ and $D_u \subset \theta_{\mathfrak{a}(x)}$, for a certain x on Γ, are equivalent by Lemma 3. (i) is thereby proved.

When u is a generic point of J over K, u is not a point of $W^* \oplus D^-$. Hence D_u and W^* have no common point by Lemma 3, and $\mathfrak{a} = 0$; (ii) is thereby proved.

We have

$$(1) \quad (((\alpha'(C)_u \times \Gamma) \cdot X) \cdot (\alpha'(C)_u \times x))_{\alpha'(C) \times \Gamma} = ((\alpha'(C)_u \times \Gamma) \cdot X) \cdot (J \times x)$$
$$= ((\alpha'(C)_u \times \Gamma) \cdot (X \cdot (J \times x)) = (\alpha'(C)_u \times \Gamma) \cdot (\theta_{\mathfrak{a}(x)} \times x) = \alpha'(C)_u \cdot \theta_{\mathfrak{a}(x)} \times x$$

by Weil [6], Chap. VII, Cor., Th. 18, Chap. VII, Th. 10, and Chap. VI, Th. 11. Hence

$$S(\alpha(\mathfrak{n})) = S(\alpha'(C)_u \cdot \theta_{\mathfrak{a}(x)}) = g \cdot u + S(\alpha'(C) \cdot \theta'_{-d+\mathfrak{a}(x)-u})$$
$$= (g-1) \cdot u - d + \alpha(x) + S(\alpha'(\mathfrak{k}'))$$

by Weil [7], Th. 20. (iii) is thereby proved.

LEMMA 6. *$(\alpha'(C)_u \times \Gamma) \cdot X^g$ is defined if and only if $\alpha(\Gamma)_{-u-d}$ is not contained in $V^- = V^*_{-S(\alpha'(\mathfrak{k}'))}$, and when that is so, a point x of Γ is a component of $\mathfrak{b}$ if and only if $\alpha(x)$ is a component of $\alpha(\Gamma) \cap V^-_{u+d}$. In other words, x on Γ is a component of $\mathfrak{b}$ if and only if*

$$\alpha(x) + (g-1) \cdot u + S(\alpha'(\mathfrak{k}')) - d \in V^*_{g \cdot u}.$$

Proof. First, let us show that $\alpha'(C)_u \times x$ is contained in X if and only if $\alpha(x) \in V^-_{u+d}$. By the formula (1), we have

$$\alpha'(C)_u \times \Gamma \cap X \cap \alpha'(C)_u \times x = (\alpha'(C)_u \cap \theta_{\mathfrak{a}(x)}) \times x.$$

Hence $\alpha'(C)_u \times x$ is contained in X if and only if $\alpha'(C)_u \subset \theta_{\alpha(x)}$. $\alpha'(C)_u$ is a subvariety of $\theta_{\alpha(x)}$ if and only if u is on $V_{-d+\alpha(x)}$ by (ii), Lemma 3. u is a point of $V_{-d+\alpha(x)}$ if and only if $\alpha(x)$ is a point of V^-_{u+d}, and our assertion is proved.

$(\alpha'(C)_u \times \Gamma) \cdot X$ is defined if and only if $\alpha'(C)_u \times \Gamma$ is not contained in X and this is so if and only if $\alpha(\Gamma)$ is not contained in V^-_{u+d} by what we have observed. Our lemma is thereby proved.

LEMMA 7. *Let Γ be non-hyperelliptic, U be a subvariety of W^* and assume that U contains a generic point of W^* over k. Let K be a field of definition for U and x be a generic point of Γ over K. Then $X^{g-1} \cdot (U_{-\alpha(x)} \times \Gamma)$ is defined and can be written as $T + U_{-\alpha(x)} \times \mathfrak{q}(x) + Y$, where every component of T has the projection $U_{-\alpha(x)}$ on $U_{-\alpha(x)}$ and Γ on Γ and the projection of every component of Y on $U_{-\alpha(x)}$ is a proper subvariety of $U_{-\alpha(x)}$. Then there is an irrational pencil Σ, free from fixed components, defined over K on Γ such that $x + \mathfrak{q}(x) = m \cdot \mathfrak{p} + \mathfrak{c}$, where m is a positive integer, $\mathfrak{p}$ is a generic member of Σ over K and $\mathfrak{c}$ is a positive rational divisor of Γ over K.*

Proof. Since U is a subvariety of W^*, it follows that $U_{-\alpha(x)}$ is a subvariety of θ by Lemma 1. Moreover, since U contains a generic point of W^* over k, it follows that $U_{-\alpha(x)}$ contains a generic point of θ over k by Lemma 1. It is clear that $X^{g-1} \cdot (U_{-\alpha(x)} \times \Gamma)$ is defined and that $x + \mathfrak{q}(x)$ is rational over $K(x)$. Let x' be a generic point of Γ over K and put $X \cdot (U_{-\alpha(x')} \times \Gamma) = T' + U_{-\alpha(x')} \times \mathfrak{q}(x') + Y'$. Let s be a generic point of U over $K(x, x')$. Then we have

$$s = S(\alpha(T(s - \alpha(x)) + \mathfrak{q}(x) + x)) = S(\alpha(T'(s - \alpha(x')) + \mathfrak{q}(x') + x')),$$

and therefore, we have

$$T(s - \alpha(x)) + \mathfrak{q}(x) + x \sim T'(s - \alpha(x')) + \mathfrak{q}(x') + x'$$

by Weil [7], Th. 19. Since s is a generic point of W^* over k by our assumption, it follows that $l(T(s - \alpha(x)) + \mathfrak{q}(x) + x) = 2$ by Lemma 1, Appendix; since $\mathfrak{L}(T(s - \alpha(x)) + \mathfrak{q}(x) + x)$ is defined over the algebraic closure of $K(s)$, and since x is a generic point of Γ over $K(s)$, it follows that the divisor $T(s - \alpha(x)) + \mathfrak{q}(x) + x$ is a generic divisor of $\mathfrak{L}(T(s - \alpha(x)) + \mathfrak{q}(x) + x)$ over $\overline{K(s)}$. Assume that x' is a component of $\mathfrak{q}(x) + x$, which is not algebraic over K. Then x' is a generic point of Γ over $K(s)$ and therefore

$$T(s - \alpha(x)) + \mathfrak{q}(x) + x = T'(s - \alpha(x')) + \mathfrak{q}(x') + x'.$$

$K(x)$ and $K(x')$ have the same algebraic closure $\overline{K(x)}$, $T(s - \alpha(x))$ and

$T'(s-\alpha(x'))$ consist of generic points of Γ over $\overline{K(x)}$ and $\mathfrak{q}(x)+x$, $\mathfrak{q}(x')+x'$ are both rational over $\overline{K(x)}$. Therefore $x+\mathfrak{q}(x)=x'+\mathfrak{q}(x')$. Let z be the Chow-point of $x+\mathfrak{q}(x)$; z is rational over $K(x)$ and hence z has a locus Z over K. Let f be the rational mapping of Γ onto Z such that $f(x)=z$. When x' is a component of $x+\mathfrak{q}(x)$, which is not algebraic over K, then $f(x')=z$ by what we have seen. Hence $x+\mathfrak{q}(x)=m\cdot f^{-1}(z)+\mathfrak{c}$, where m is a positive integer and $\mathfrak{c}$ is a fixed rational divisor over K (cf. Weil [6], Chap. VI, Th. 11).

In order to complete our lemma, it is sufficient to prove that Z is not a rational curve. If Z is a rational curve, then $x+\mathfrak{q}(x)\sim x'+\mathfrak{q}(x')$ whenever x and x' are two independent generic points of Γ over K. Therefore $T(s-\alpha(x))\sim T'(s-\alpha(x'))$. Since $U_{-\alpha(x)}$ contains a generic point of θ over k, $s-\alpha(x)$ is a generic point of θ over k and consequently $T(s-\alpha(x))+\mathfrak{q}(x)$ is a generic divisor on Γ of degree $g-1$ over k. Hence $T(s-\alpha(x))\sim T'(s-\alpha(x'))$ if and only if $T(s-\alpha(x))=T'(s-\alpha(x'))$. When x and x' are independent generic points of Γ over $K(s)$, then $T(s-\alpha(x))+\mathfrak{q}(x)+x$ and $T'(s-\alpha(x'))+\mathfrak{q}(x')+x'$ are two independent generic divisors of the pencil $\mathfrak{L}(T(s-\alpha(x))+\mathfrak{q}(x)+x)$ over the algebraic closure of $K(s)$. Therefore, if $T(s-\alpha(x))=T'(s-\alpha(x'))$, then $T(s-\alpha(x))$ is a fixed divisor of the pencil, which is contrary to our hypothesis that Γ is not hyperelliptic (cf. Lemma 1, Appendix). Our lemma is thereby proved.

3. LEMMA 8. *Let t and u be generic points of $W^*\oplus\alpha'(C)^-$ and $W^*\oplus\alpha'(C)$ over k. Put $(\alpha'(C)_t\times\Gamma)\cdot X^g=T+\alpha'(C)_t\times\mathfrak{b}+\mathfrak{a}\times\Gamma$, and also*

$$(\alpha'(C)^-_u\times\Gamma)\cdot X^g=T'+\alpha'(C)^-_u\times\mathfrak{b}'+\mathfrak{a}'\times\Gamma.$$

When Γ is not a hyperelliptic curve, either $\deg(\mathfrak{b})=1$ *or* $\deg(\mathfrak{b}')=1$.

Proof. By Lemmas 3 and 6, $\mathfrak{b}$ and $\mathfrak{b}'$ are not 0. Assume that $\deg(\mathfrak{b})>1$. Write $\mathfrak{b}=\sum_1^s c_i$ and put $v=S(\alpha(\mathfrak{k}))-t+\alpha(c_{s-1})+\alpha(c_s)$. $\alpha'(C)^-_v$ contains a generic point of W^* over k an dis contained in it. In fact, putting $K=\overline{k(t)}$, a generic point of $\alpha'(C)_t$ over K is a generic point of J over k. Therefore, when we write a generic point of $\alpha'(C)_t$ over K in the form

$$S(\alpha(\textstyle\sum_1^{g-s}(x_i)+\sum_1^s(c_i))),$$

$(x_1,\cdots,x_{g-s},c_1,\cdots,c_s)$ is a set of g independent generic points of Γ over k. When that is so, $S(\alpha(\mathfrak{k}-\sum_1^{g-s}(x_i)-\sum_1^{s-2}(c_i)))$ is a generic point of W^* over k by the definition of W^*. Our assertion is thereby proved.

Let y_1 and y_2 be two independent generic points of Γ over K. Put $z = v - \alpha(y_1) + \alpha(y_2)$ and

$$(\alpha'(C)^-_z \times \Gamma) \cdot X^g = T'' + \alpha'(C)^-_z \times \mathfrak{b}'' + \mathfrak{a}'' \times \Gamma.$$

We shall show that $\mathfrak{b}'' = y_2$, which is sufficient to prove our lemma (cf. Lemmas 3 and 6). Since $\alpha'(C)^-_v$ contains a generic point of W^* over k and is contained in it, we may apply Lemma 7 to this curve. Let $\bar{X}$ be the subvariety X^{g-1} on $\theta \times \Gamma$ defined in no. 2. Since $\alpha'(C)^-_{v-\alpha(y_1)}$ contains a generic point of θ over K and is contained in it by Lemma 1, $\alpha'(C)^-_{v-\alpha(y_1)} \times \Gamma$ is not a subvariety of $\bar{X}$. Therefore $\bar{X} \cdot (\alpha'(C)^-_{v-\alpha(y_1)} \times \Gamma)$ is defined. Put

$$\bar{X} \cdot (\alpha'(C)^-_{v-\alpha(y_1)} \times \Gamma) = \bar{T} + \alpha'(C)^-_{v-\alpha(y_1)} \times \mathfrak{b} + \mathfrak{a} \times \Gamma,$$

and $\mathfrak{b} = \mathfrak{q}(y_1)$. Let Σ be the set of specializations of $y_1 + \mathfrak{q}(y_1)$ over K, then by our Lemma 7, Σ is an irrational pencil. Next, we claim that Σ is free from fixed components. Let r be a generic point of $\alpha'(C)^-_v$ over $K(y_1)$, then $r = S(\alpha(\bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1))$. Since r is a generic point of W^* over k and since

$$\deg(\bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1) = g,$$

$\mathfrak{m} = \bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1$ is a generic divisor of $\mathfrak{L}(\mathfrak{m})$ over the algebraic closure of $K(r)$. Since $\mathfrak{L}(\mathfrak{m})$ has no fixed component by Lemma 1, Appendix, it follows that $\mathfrak{q}(y_1)$ cannot contain a component which is algebraic over $K(r)$. Hence our assertion is proved.

By Lemma 3, Appendix, Σ is defined over $\bar{k}$, and hence $S(\alpha(\mathfrak{q}(y_1) + y_1)) = a$ is a constant, which is independent with respect to v over k. Assume that $\mathfrak{q}(y_1)$ is not empty, then $\deg(y_1 + \mathfrak{q}(y_1)) = m > 1$ and $\alpha'(C)^-_v$ is contained in W^{g-m}_a. Since $\alpha'(C)^-_v$ contains a generic point of W^* over k, we must have $m \leqq 2$. When $m = 2$, we have $W^{g-2}_a = W^*$ and this is possible if and only if $l(y_1 + \mathfrak{q}(y_1)) > 1$ by the theorem of Riemann-Roch. This contradicts our hypothesis that Γ is not a hyperelliptic curve. Thus $m = 1$ and $\mathfrak{q}(y_1) = 0$. From this we see immediately that $\mathfrak{b}'' = \alpha(y_2)$ and our lemma is thereby proved.

4. THEOREM (hyperelliptic case). *Let Γ and C be two complete non-singular hyperelliptic curves of genus g. Let J (resp. J') be the Jacobian variety of Γ (resp. C) and α (resp. α') be the canonical mapping of Γ (resp. C) into J (resp. J'). Assume that there is an isomorphism of β of J into J' such that canonical divisors θ and θ' on J and J' with respect to Γ*

and C satisfy $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Then there is a birational transformation h of Γ onto C such that

$$\alpha' \cdot h = \pm \beta \cdot \alpha + \text{constant};$$

we can select $+$ or $-$ arbitrarily, but if it is once selected, h and the constant are uniquely determined by β.

Proof. We make the identification stated in the beginning of this paper. Let $\mathfrak{c}$ (resp. $\mathfrak{c}'$) be a positive divisor of degree 2 on Γ (resp. C) such that $l(\mathfrak{c})$ (resp. $l(\mathfrak{c}')$) > 1. Since $\theta' = \theta_d$, we may assume that $\theta = \theta'$ by adding a suitable constant to α'. By the proposition in our Appendix, a point u of $\mathfrak{k}$ is a singular point of θ if and only if a positive Γ-divisor $\mathfrak{m}$ of degree $g-1$ such that $S(\alpha(\mathfrak{m})) = u$ satisfies $l(\mathfrak{m}) > 1$. When that is so, $l(\mathfrak{m}-\mathfrak{c})$ is positive and this shows that u is a point of $W^{g-3}{}_s$, where $s = S(\alpha(\mathfrak{c}))$. Conversely, it is clear that any point of $W^{g-3}{}_s$ is a singular point of θ by the same proposition. When we put $s' = S(\alpha'(\mathfrak{c}'))$, $V^{g-3}{}_{s'}$ is also the set of singular points of $\theta' = \theta$ and hence we have $W^{g-3}{}_s = V^{g-3}{}_{s'}$.

It is easy to see that $W^* = W^{g-2}{}_s$, $V^* = V^{g-2}{}_{s'}$ (cf. Weil [7], Prop. 16). Let t be a generic point of $W^* \oplus \alpha'(C)^-$ over $K = k(s, s')$. By Lemma 3, t can be written as $v + \alpha(x)$, where v and x are independent generic points of V and Γ over K. By the same lemma, $\alpha'(C)_v \cap W^*{}_{-\alpha(x)}$ is not empty. *We shall show that it contains at least $g-1$ distinct points.* A generic point of $W^*{}_{-\alpha(x)}$ over $K(x)$ can be written as $S(\alpha'(\sum_1^{g-1} y_i))$ where the y_i are points on C, and $g-2$ points among $(y_1, \cdots, y_{g-1})$, say $(y_1, \cdots, y_{g-2})$, are independent generic points of C over $K(x)$. Put $v' = S(\alpha'(\sum_1^{g-2} y_i))$; then v' is a generic point of V over $K(x)$ and $\alpha'(C)_{v'}$ contains a generic point of θ over K, which is a generic point of $W^*{}_{-\alpha(x)}$ over $K(x)$. Since v and v' are generic specializations of each other over $K(x)$, $\alpha'(C)_v$ also has the same properties. Hence $\alpha'(C)_v \cdot W^*{}_{-\alpha(x)}$ is defined on θ and is not empty. Identifying v and v', let y'_i be the point on C such that $y_i + y'_i \sim \mathfrak{c}'$. Then $\alpha'(y'_i) + v$ is on $\alpha'(C)_v$ and $V^{g-3}{}_{s'} = W^{g-3}{}_s$. Thus $\alpha'(y'_i) + v = S(\alpha(\mathfrak{m}_i))$, where $\mathfrak{m}_i$ is a positive Γ-divisor of degree $g-1$; since $l(\mathfrak{m}_i) > 1$, $\mathfrak{m}_i \sim x' + \mathfrak{n}_i$, where x' is the point on Γ such that $x + x' \sim \mathfrak{c}$ and $\mathfrak{n}_i$ is a positive Γ-divisor of degree $g-2$. It follows that $\alpha'(y'_i) + v \in W^{g-2}{}_{\alpha(x')} = W^*{}_{-\alpha(x)}$. It is clear that when $i \neq j$, $\alpha'(y'_i) + v \neq \alpha'(y'_j) + v$. $\alpha'(y'_i) + v$ is a singular point of θ by the proposition in our Appendix. Thus our assertion is proved.

Since t is a generic point of $W^* \oplus \alpha'(C)^-$ over K, $\alpha'(C)_t$ is not contained in W^*. Therefore $(\alpha'(C)_t \times \Gamma) \cdot X^g$ is defined and can be written in the form $T + \mathfrak{a}' \times \Gamma + \alpha'(C)_t \times \mathfrak{b}$. By (i), Lemma 5, we

have $\deg(\mathfrak{a}') \geqq g-1$. If $\deg(\mathfrak{a}') = g$, then $T = 0$, $\deg(\mathfrak{b}) = g$ by the formula (1) and this is impossible from the definition of X and Weil [7], Th. 19. Hence we must have $\deg(\mathfrak{a}') = g-1$, and since $(\alpha(C)_t \times \Gamma) \cdot X$ is a correspondence of type (g, g) by the formula (1), it follows that T is the graph of a rational mapping $\bar{h}$ of Γ onto $\alpha'(C)_t$. Since a generic point $\alpha'(y) + t$ of $\alpha'(C)_t$ over $K(t)$ is a generic point of J over K, every component of $T(\alpha'(y) + t)$ has the coefficient 1, which proves that $\bar{h}$ is a separable mapping. By Lemma 2, Appendix, $\bar{h}$ is then a birational transformation, and we have $\alpha'(y) + t = \alpha(\bar{h}^{-1}(\alpha'(y) + t)) + S(\alpha(\mathfrak{b}))$. Thus we see that $\alpha'(C) = \alpha(\Gamma)_c$, where c is a constant, and that there is a birational transformation h of Γ onto C such that $\alpha(x) = \alpha'(h(x)) + c'$, where c' is a constant. Let f' be the birational transformation of C onto itself such that whenever y is a point of C, $y + f'(y) \sim \mathfrak{c}'$. Then since $\alpha'(h(x)) + \alpha'(f' \cdot h(x)) = S(\alpha'(\mathfrak{c}'))$, we see that $\alpha(x) = -\alpha'(f' \cdot h(x)) + c''$, where c'' is a constant. Since $\mathfrak{L}(\mathfrak{c})$ is uniquely determined on Γ, h is determined uniquely by the relation $\alpha = \alpha' \cdot h +$ constant; in the same way, $f' \cdot h$ is uniquely determined by the relation $\alpha = -\alpha' \cdot (f' \cdot h) +$ constant. Our theorem is thereby proved.

THEOREM (non-hyperelliptic case). *Let Γ and C be two complete non-singular curves of the same genus g and assume that one of the two curves is not a hyperelliptic curve. Let J (resp. J') be the Jacobian variety of Γ (resp. C) and α (resp. α') be the canonical mapping of Γ (resp. C) into J (resp. J'). Assume that there is an isomorphism β of J onto J' such that canonical divisors θ and θ' on J and J' with respect to Γ and C satisfy $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Then there is a birational transformation h of Γ to C such that*

$$\alpha' \cdot h = \pm \beta \cdot \alpha + \text{constant},$$

where the signature, h and the constant are uniquely determined by β.

Proof. As in the proof of the preceding theorem, we make the identification $J = J'$, as stated in the beginning of this paper. For the sake of simplicity, let us assume that Γ is not hyperelliptic. Then by Lemma 8, either $\alpha'(C)$ or $\alpha'(C)^-$ satisfies the property described in the Lemma. Assume that $\alpha'(C)$ satisfies it, i.e. letting t be a generic point of $W^* \oplus \alpha'(C)^-$ over k, and writing $(\alpha'(C)_t \times \Gamma) \cdot X^g = T + \mathfrak{a}' \times \Gamma + \alpha'(C)_t \times \mathfrak{b}$, assume that $\deg(\mathfrak{b}) = 1$. By Lemma 6, when we put $v = -t - d + S(\alpha'(\mathfrak{k}'))$, $\alpha(\Gamma)$ and V^* have just a single point in common. Then v is a generic point of $V^* \oplus \alpha(\Gamma)^- = W_d \oplus \alpha'(C)$ over k by Lemma 3, and can be written as $v = w + \alpha'(y) + d$, where w and y are independent generic points of W and

C over k. Thus we see that $V^*_{-\alpha'(y)}$ and $\alpha(\Gamma)_{w+d}$ have just a single point in common. It is easy to see that we have

$$\theta' \cap \theta'_{\alpha'(z)-\alpha'(y)} = V_{\alpha'(z)} + V^*_{-\alpha'(y)},$$

by Lemma 1, by the theorem of Riemann-Roch and by the definitions of V and V^* (cf. also Weil [7], Prop. 16), where z is a generic point of C over $k(w,y)$. Since $\alpha(\Gamma)_{w+d}$ is contained in $\theta_d = \theta'$ and since $\alpha'(z) - \alpha'(y) - w$ is a generic point of J over k, it follows that $V_{\alpha'(z)}$ and $\alpha(\Gamma)_{w+d}$ have at least $g-1$ distinct points in common by Weil [7], Th. 20. Thus we have shown that when we put $u = w + d - S(\alpha'(\mathfrak{k}')) - \alpha'(z)$, $V_{-S(\alpha'(\mathfrak{k}'))}$ and $\alpha(\Gamma)_u$ have at least $g-1$ distinct points in common.

Put $D = \alpha'(C)^-$. Then J is the Jacobian variety of D, the injection map of D into J is the canonical mapping of D into J and θ'^- is the set of sums of $g-1$ points on D. Let X' be the subvariety of $J \times D$ with a field of definition k such that when s is a generic point of J over k, $X'(s) = \mathfrak{m} \succ 0$, $\deg(\mathfrak{m}) = g$ and $s = S(\mathfrak{m})$. Then $V_{-S(\alpha'(\mathfrak{k}'))}$ is the set of classes of special D-divisors of degree g. By Lemma 4, $(\alpha(\Gamma)_u \times D) \cdot X'$ is defined. By (i), Lemma 5, we see that, in the expression

$$(\alpha(\Gamma)_u \times D) \cdot X' = T_1 + \mathfrak{a} \times D + \alpha(\Gamma)_u \times \mathfrak{b}_1,$$

we must have $\deg(\mathfrak{a}) \geqq g-1$. Since $(\alpha(\Gamma)_u \times D) \cdot X'$ is a correspondence of type (g,g) on $\alpha(\Gamma)_u \times D$ by the formula (1), $\deg(\mathfrak{a}) = g$ implies $T' = 0$ and $\deg(\mathfrak{b}_1) = g$, which is impossible because of the definition of X' and Weil [7], Th. 19. Hence $\deg(\mathfrak{a}) = g-1$ and T_1 is the graph of a rational mapping of D onto $\alpha(\Gamma)_u$. Since $\dim_k(u) = g-1$, $\alpha(\Gamma)_u$ contains a generic point of J over k. It follows that when $\alpha(x) + u$ is a generic point of $\alpha(\Gamma)_u$ over $k(u)$, then it is a generic point of J over k, and every component of $T_1(\alpha(x) + u)$ has the coefficient 1. Therefore T_1 is the graph of a separable rational mapping f. When that is so, f is a birational mapping by Lemma 2 of the Appendix. Now let us assume that $-\alpha'(y)$ is a generic point of D over $k(u)$; then we have

$$S(f(-\alpha'(y)) + \mathfrak{a}) = -\alpha'(y) + (g-1)u + S(\alpha(\mathfrak{k})) + d + S(\alpha'(\mathfrak{k}')),$$

by (iii), Lemma 5 (Remark: $\theta'^- = \theta^-_{-d} = \theta_{-S(\mathfrak{a}(\mathfrak{k}))-d}$). Thus we have seen that $\alpha(\Gamma) = D_c = \alpha'(C')^-_c$, where c is a constant rational over $k(u)$. Let h be the birational transformation of Γ to C such that $-\alpha' \cdot h + c = \alpha$; then h is the one we are looking for.

Let h' be a rational transformation of Γ to C such that $\alpha' \cdot h' = \alpha + c'$,

where c' is a constant, and let K be a common field of definition for h and h'. Let x be a generic point of Γ over K; then we see that $\alpha'(h(x)) + \alpha'(h'(x)) = \text{constant}$, which implies that $l(h(x) + h'(x)) > 1$ by Weil [7], Th. 19. Since C cannot be a hyperelliptic curve by what we have proved, there exists no such h'. If we have $-\alpha' \cdot h' = \alpha + c'$, then $h(x) + h'(x') = h(x') + h'(x)$ for any two points x and x' on Γ by the same reason as before, which shows that $h(x) = h'(x)$, i.e. $h = h'$. Our theorem is thereby proved.

Appendix.

1. A complete non-singular curve C is called *hyperelliptic*, if it carries a positive divisor $\mathfrak{a}$ of degree 2 such that $l(\mathfrak{a}) > 1$.

LEMMA 1. *Let C be a complete non-singular curve of genus g, J be its Jacobian variety and α be the canonical mapping of C into J. Let k be a common field of definition for C, J, α and let $\mathfrak{m}$ be a positive C-divisor of degree g such that $S(\alpha(\mathfrak{m}))$ is a generic point of W^* over k. Then $l(\mathfrak{m}) = 2$; and when C is not a hyperelliptic curve, $\mathfrak{L}(\mathfrak{m})$ is a linear pencil without fixed point.*[2]

Proof. Let F be the rational mapping of the product U of g curves equal to C into J, which is defined by $F(x_1, \cdots, x_g) = \alpha(x_1) + \cdots + \alpha(x_g)$. We have $\dim W^* = g - 2$ and $l(\mathfrak{m}) > 1$ by Weil [7], Prop. 16. If $l(\mathfrak{m}) > 2$, there must be a generic point $(y_1, \cdots, y_g)$ of U over k such that $F(y_1, \cdots, y_g)$ is $S(\alpha(\mathfrak{m}))$ by Weil [7], Th. 19 and this is impossible. Hence $l(\mathfrak{m}) = 2$.

By definition of W^*, there is a set $(z_1, \cdots, z_{g-2})$ of $g-2$ independent generic points of C over k such that $\mathfrak{m} \sim \mathfrak{k} - \sum_1^{g-2}(z_i)$, where $\mathfrak{k}$ is a canonical divisor on C. Put $\mathfrak{m} = \sum_1^g(t_i)$, assume that $\mathfrak{L}(\mathfrak{m})$ has a fixed point and let r be the smallest non-negative integer such that $\mathfrak{k} - \sum_1^r(z_i)$ defines a complete linear system with a fixed point z'. Then z' is algebraic over $k(z_1, \cdots, z_r)$, but not algebraic over the field generated by an subset of $(z_1, \cdots, z_r)$ over k. Let z_{g-1} be a generic point of C over $k(z_1, \cdots, z_{g-2})$. Since $l(\mathfrak{k}) = g$, with any subset $(z_{i_1}, \cdots, z_{i_r})$ of $(z_1, \cdots, z_{g-1})$ we can associate the set of fixed points (z'_i) of the complete linear system $\mathfrak{L}(\mathfrak{k} - (z_{i_1}) - \cdots - (z_{i_r}))$; what we have observed shows that if $(z_{i_1}, \cdots, z_{i_r})$ and $(z_{j_1}, \cdots, z_{j_r})$ are different as sets, then (z'_i) and (z'_j) have no point in

[2] The writer owes the proof of the latter half of this lemma to M. Rosenlicht.

common. Let s be the number of points in the set (z'_i), which is independent of i. Then we have

$$(g-1)+s\cdot\binom{g-1}{r}\leqq \deg(\mathfrak{k})=2g-2.$$

Therefore we have $r=1$ or $g-2$ and $s=1$. When $r=1$, C is a hyperelliptic curve which we have excluded. Thus we have $r=g-2$ and $s=1$. Let z' be the fixed point of $\mathfrak{L}(\mathfrak{k}-\sum_1^{g-2}(z_i))$, then it is easy to see that z' is rational over $k(z_1,\cdots,z_{g-2})$ (cf. Weil [6], Chap. VIII, Th. 10), which we shall write $z'=f(z_1,\cdots,z_{g-2})$. f is then a symmetric function defined on $C\times\cdots\times C$ ($g-2$ factors) with values in C defined over k and we have

$$\mathfrak{k}\sim\sum_1^{g-1}(z_i)+\sum_j f(z_1,\cdots,z_{j-1},z_{j+1},\cdots,z_{g-1}).$$

By Weil [7], Cor., Th. 7, $\alpha f(z_1,\cdots,g_{g-2})=\sum_i h(z_i)+\text{constant}$, where h is a function defined on C with values in J. Let γ be the linear extension of h, i.e. the endomorphism of J such that $h=\gamma\cdot\alpha+\text{constant}$ (cf. Weil [7], Th. 21). We have $\alpha\cdot f(z_1,\cdots,z_{g-2})=\sum_i\gamma\cdot\alpha(z_i)+\text{constant}$ and

$$S(\alpha(\mathfrak{k}))=\sum_1^{g-1}\alpha(z_i)+(g-2)\cdot\sum_1^{g-1}\gamma\cdot\alpha(z_i)+\text{constant}.$$

Therefore $\alpha(z_i)+(g-2)\cdot\gamma\cdot\alpha(z_i)=c_i$, where c_i is a constant rational over k, since h and γ are defined over k (cf. Weil [7], Cor., Th. 7 and Th. 21). Now let $z_1,\cdots,z_g$ be g independent generic points of C over k. Then we have

$$k(z_1,\cdots,z_g)_s=k(\alpha(z_1)+\cdots+\alpha(z_g))=k((g-2)\cdot\textstyle\sum\gamma\cdot\alpha(z_i)),$$

which is only possible when $g=3$ (cf. Weil [7], Th. 18). When $g=3$, then we have $r=1$ and our C is a hyperelliptic curve. Our lemma is thereby proved.

Let h be a rational mapping of a variety V onto another variety V'. Let k be a common field of definition for V, V' and h and let x be a generic point of V over k. We say that h is a *separable* (resp. *regular*) *mapping* when $k(x)$ is a separably generated (resp. regular) extension of $k(h(x))$.

LEMMA 2. *Let C and C' be two complete non-singular curves of the same genus and assume that there is a separable rational mapping h from C to C'. Then h is a birational transformation.*

Proof. Let J and J' be the Jacobian varieties of C and C'. We may assume, without loss of generality, that canonical mappings from both curves into their Jacobian varieties are injections. Then the linear extension β of h (cf. Weil [7], Th. 21) is a surjective homomorphism of J to J'. Assume

that h^{-1} is not a rational mapping; then the kernel of β does not consist of the neutral element O only. Suppose that the kernel of β consists of a finite set of points $O, a_1, \cdots, a_s$. Let x and y be two generic points of C over a field k of definition for C, C', J, J', h and β. Then $\beta(x) = \beta(y)$ when $h(x) = h(y)$; when that is so, we have $y = x + a_i$ for some i (putting $a_0 = O$). In this case, we have $C = C_{a_i}$ and hence $\theta = \theta_{a_i}$, where θ is the theta-divisor on J corresponding to C. On the other hand, we have $\theta = \theta_t$ if and only if $t = O$ by Weil [7], Cor. 3, Th. 30. Therefore, the kernel of β must form an algebraic subgroup of J of dimension greater than 0. This contradicts our hypothesis that C and C' have the same genus.

Let V be a complete variety, non-singular in co-dimension 1. Let F be a rational mapping of V onto a complete non-singular curve C; then we say that (F, C) defines on V a *pencil of divisors* which consists of $F^{-1}(u)$ with u on C. It is called *linear* when C is a rational curve. When C is a curve of genus g, it is called an *irrational pencil of genus g*. There is a classical theorem, saying that there cannot be an algebraic family of irrational pencils on a curve, which is due to Humbert and Castelnuovo. We shall generalize this theorem to varieties of higher dimension.

LEMMA 3. *Let V be a complete variety, non-singular in co-dimension 1 and let Z be a subvariety of a product $U \times W \times V$. Let k be an algebraically closed common field of definition for V, U, W and Z and assume that, when u is a generic point of U over k, $Z(u)$ is the gfaph of a rational mapping F_u of V onto a complete non-singular curve C_u contained in W. Let v be a generic point of U over $k(u)$, then unless C_u (and consequently C_v) is not a rational curve, (F_u, C_u) and (F_v, C_v) define on V the same irrational pencil.*

Proof. We may assume, without loss of generality, that V is a projective variety. First we shall show that our question can be reduced to the case of curves. Let H be a generic hypersurface over $k(u, v)$. By Weil [6], Chap. V. Prop. 2, Chap. VII, Cor., Th. 10 and Chap. VII, Th. 17, $Z \cdot (U \times W \times V \cdot H)$ is defined, irreducible,

$$(Z \cdot (U \times W \times V \cdot H)) \cdot (u \times W \times V) = (u \times Z(u)) \cdot (U \times W \times V \cdot H),$$

which also can be written as $u \times (W \times V \cdot H) \cdot Z(u)$, is prime rational over the smallest common field of definition for u and H containing k and has the projection C_u on W. Let x be a generic point of V over $k(u, v)$ and put $X = F_u^{-1}(F_u(x))$, $Y = F_v^{-1}(F_v(x))$. Let $\mathfrak{L}_m$ be the linear system of sections of V by hypersurfaces of order m. If m is sufficiently large, $\dim \mathfrak{L}_m \geqq 3$ and

the linear subsystem of $\mathfrak{L}_m$, consisting of divisors going through x, induces on any component T of X and Y a linear system of dimension at least 1. Let H_m be a generic hypersurface of order m over $k(u,v,x)$ going through x. Then clearly H_m is a generic hypersurface of order m over $k(u,v)$; moreover, $X\cdot H_m$ and $Y\cdot H_m$ are defined by our choice of $\mathfrak{L}_m$. Since $T\cdot H_m$ is rational over a field of transcendence degree at least 1 over $k(u,v,x)$ by our choice of $\mathfrak{L}_m$, it contains a generic point of T over the algebraic closure of $k(u,v,x)$. By the formula we have shown in the beginning of our proof, if our lemma is true for $V\cdot H_m$, i.e. if $F_u^{-1}(F_u(x))\cdot H_m = F_v^{-1}(F_v(x))\cdot H_m$, then what we have observed in the preceding discussion shows that $F_u^{-1}(F_u(x)) = F_v^{-1}(F_v(x))$. Repeating this process, we see that our lemma is true whenever it is true on a complete non-singular curve Γ in a projective space, since $V\cdot H_m$ is again complete and non-singular (cf. Zariski [11]; Nakai [3]).

Let J be the Jacobian variety of Γ, α be the canonical mapping of Γ into J and K be a common field of definition for J, Γ and α. Let u be a generic point of U over K and t be a generic point of C_u over $K(u)$. Put $F_u^{-1}(t) = \mathfrak{m}$, $S(\alpha(\mathfrak{m})) = s$. Then when x and y are components of $\mathfrak{m}$, we see that s is rational over $K(x)$ (cf. Weil [6], Chap. VI, Th. 12; Weil [7], Th. 1) and that the rational mapping f_u of Γ into J defined by $f_u(x) = s$ is such that $f_u(y) = s$. f_u can be written as $\beta\cdot\alpha + c_u$, where β is an endomorphism of J and c_u is a constant, both defined over $K(u)$ by Weil [7], Th. 21. Since there is no algebraic family of endomorphisms on an abelian variety (Chow [2]), β is actually defined over K. Assume that $\deg(\mathfrak{m}) \geqq 2$ and that the pencil defined on Γ by (F_v, C_v) is different from the pencil defined by (F_u, C_u); in other words, assume that $F_u^{-1}(F_u(x)) \neq F_v^{-1}(F_v(x))$. Then $\mathfrak{m}$ cannot be algebraic over $K(x)$ and hence the field generated over K by components of $\mathfrak{m}$ has at least the dimension 2 over K. Therefore we may assume that $\dim_K(x,y) = 2$. $f_u(x) = f_v(y)$ implies $\beta = 0$ and thus (F_u, C_u) defines on Γ a linear pencil by Weil [7], Th. 19. Consequently, we have

$$Z(u) \sim \mathfrak{a}\times\Gamma + C_u\times\mathfrak{m},$$

where $\deg(\mathfrak{a}) = 1$. Since $Z(u)$ is the graph of a rational mapping of Γ onto C_u, it follows that $t \sim t'$ for any two point on C_u by Weil [6], Chap. VIII, Cor. 1, Th. 4. Thus C_u must be a rational curve. When $\deg(\mathfrak{m}) = 1$, our lemma is trivial and the proof is completed.

2. LEMMA 4. *Let U be a product of n complete non-singular curves Γ_i; let F be a rational mapping of U onto a variety T^n. Let $u = (x_1, \cdots, x_n)$*

be a point on U and denote by $R(i_1, \cdots, i_r)$ the subvariety of U which we get by replacing the i_j-th factor Γ_{i_j} by x_{i_j} for $1 \leqq j \leqq r$ (we assume always that $i_1 < \cdots < i_r$). Assume that F is defined at u, $F(u)$ is simple on T and that the graph of F is transversal to $U \times F(u)$ at $u \times F(u)$ on $U \times T$. Assume also that $F(u)$ is simple on the image $R(i_1, \cdots, i_r)^*$ of $R(i_1, \cdots, i_r)$ by F, for any choice of $(i_1, \cdots, i_r)$. Let V^{n-r} be a subvariety of T, having $F(u)$ as a simple point. Then there is at least one $(i_1, \cdots, i_r)$ such that $R(i_1, \cdots, i_r)^*$ is transversal to V at $F(u)$ on T.

Proof. Let k be a common field of definition for the Γ_i, T, u, F and V. Let W be any subvariety of T having $F(u)$ as a simple point; then there is a subvariety H of T such that H and W are transversal to each other at $F(u)$ on T (cf. for instance Weil [6], Chap. V, Th. 5). Identifying F with its graph and applying Weil [6], Chap. VI, Th. 5 and Th. 6 to $U \times H \cap U \times W \cap F$, we see that a component $\bar{W}$ of $F \cap U \times W$ containing $u \times F(u)$ is uniquely determined, is a proper component of multiplicity 1 on $U \times T$ and has $u \times F(u)$ as a simple point.

F is defined along $R(i_1, \cdots, i_r)$ by Weil [6], Chap. IV, Cor., Th. 15. Then there is the uniquely determined subvariety $R(i_1, \cdots, i_r)'$ on F having the projection $R(i_1, \cdots, i_r)$ on U, which is a proper component of multiplicity 1 in $R(i_1, \cdots, i_r) \times T \cap F$ on $U \times T$ by Weil [6], Chap. VI, Cor., Th. 6 and Th. 8. The image $R(i_1, \cdots, i_r)^*$ of $R(i_1, \cdots, i_r)$ by F is the projection of $R(i_1, \cdots, i_r)'$ on T. When we apply the result just proved in the beginning of this proof to $F \cap U \times V$ and to $F \cap U \times R(i_1, \cdots, i_r)^*$, we see that there are the uniquely determined components $\bar{V}$ and $R(i_1, \cdots, i_r)'$ containing $u \times F(u)$ in them, and that they are proper components of multiplictiy 1 on $U \times T$, having $u \times F(u)$ as simple points. By Weil [6], Chap. VI, Th. 9, we see that

$$i(\bar{V} \cdot (U \times R(i_1, \cdots, i_r)^*), u \times F(u); U \times T)$$
$$= i(\bar{V} \cdot R(i_1, \cdots, i_r)', u \times F(u); F) = i(V' \cdot R(i_1, \cdots, i_r), u; U),$$

where V' is the projection of $\bar{V}$ on U (cf. also Weil [6], Chap. VI, Th. 8). By Weil [6], Chap. VI, Th. 5, we see also that

$$i(V \cdot R(i_1, \cdots, i_r)^*, F(u); T) = i(\bar{V} \cdot (U \times R(i_1, \cdots, i_r)^*), u \times F(u); U \times T),$$

under the assumption that $F(u)$ is a proper component of $V \cap R(i_1, \cdots, i_r)^*$ on T. Passing to representatives, we assume that U and T are affine varieties. Let $S^1{}_i$ be the tangent linear variety to Γ_i at x_i. Then the tangent linear variety to U at u is $S^n = S^1{}_1 \times \cdots \times S^1{}_n$ by Weil [6], Chap. IV, Th. 13.

Since the projection from F to U is biregular at $u \times F(u)$, u is a simple point on V' by Weil [6], Chap. IV, Cor. 1, Th. 17. Then the tangent linear variety S^{n-r} at u to V' is contained in S^n by Weil [6], Chap. IV, Prop. 23. The tangent linear variety to $R(i_1, \cdots, i_r)$ at u is of the form $S(i_1, \cdots, i_r)$ which we get by replacing the i_j-th factor of S^n by x_{i_j} for $1 \leqq j \leqq r$. Now it is clear that at least one of the $S(i_1, \cdots, i_r)$, with $i_1 < \cdots < i_r$, is transversal to S^{n-r} at u on S^n. Let $S(i_1, \cdots, i_r)$ be such; then we have

$$i(V' \cdot R(i_1, \cdots, i_r), u; U) = 1.$$

If $F(u)$ is not a proper component of $V \cap R(i_1, \cdots, i_r)^*$, then $u \times F(u)$ is not a proper component of $V' \cap R(i_1, \cdots, i_r)$ on U and our lemma is thereby proved.

We are going to apply the preceding lemma to the following proposition, which was proved recently by A. Weil (Weil [10], Th. 3) from the consideration of differential forms.

PROPOSITION. *Let J^g be the Jacobian variety of a complete non-singular curve Γ and let α be the canonical mapping of Γ into J. Then a point w' of W^r is simple on W^r if and only if a positive divisor $\mathfrak{m}$ of degree r on Γ such that $S(\alpha(\mathfrak{m})) = w'$ has the property $l(\mathfrak{m}) = 1$.*

Proof. If $l(\mathfrak{m}) = 1$, then w' is simple on W^r by Weil [7], Prop. 18. Therefore, assume that $l(\mathfrak{m}) > 1$. Let U be the product of g curves equal to Γ and let F be the rational mapping of U onto J defined by $F(x_1, \cdots, x_g) = \sum \alpha(x_i)$. Let k be a common field of definition for Γ, J, α, F, w' and let u be a generic point of J over k. Then $w' + u$ is a generic point of J over k. If w' is simple on W^r, $w' + u$ is simple on $W^r{}_u$. Applying the preceding lemma to U, J, F, $W^r{}_u$ and to a generic point $(x_1, \cdots, x_g)$ of U over k such that $\sum \alpha(x_i) = w' + u$, it follows that there is a translation $W^{g-r}{}_t$ of W^{g-r} such that $W^r{}_u$ and $W^{g-r}{}_t$ are transversal to each other at $w' + u$ on J. Hence there is a $W^{g-r}{}_v$ such that it is transversal to W^r at w' on J. There is an $\alpha(\Gamma)_s$ on $W^{g-r}{}_v$ containing w', and when that is so, w' is a simple point of $\alpha(\Gamma)_s$. Take a representative of w' and take representatives of J, $\alpha(\Gamma)_s$, $W^{g-r}{}_v$, W^r on the same affine space. Let us denote by the same letters those representatives we have chosen. Then the tangent linear variety S^1 to $\alpha(\Gamma)_s$ at w' is contained in the tangent linear variety S^{g-r} to $W^{g-r}{}_v$ at w' by Weil [6], Chap. IV, Prop. 23. Since S^{g-r} and the tangent linear variety S^r to W^r at w' are transversal to each other at w' on the tangent linear variety S to J at w', S^1 cannot be contained in S^r. Consequently, $\alpha(\Gamma)_s$ cannot be a

subvariety of W^r. Since $\alpha(\Gamma)_s$ contains w', it can be written as $\alpha(\Gamma)_{w'-\alpha(x)}$, where x is a point on Γ. For any point y on Γ, we have $l(\mathfrak{m}-x+y)\geqq 1$ and hence there is a positive divisor $\mathfrak{m}'$ of degree r on Γ such that $\mathfrak{m}'\sim\mathfrak{m}-x+y$. By Weil [7], Th. 19, we have $S(\alpha(\mathfrak{m}'))=S(\alpha(\mathfrak{m}-x+y))$, and this shows that $\alpha(\Gamma)_s$ is contained in W^r, which is a contradiction. Therefore w' cannot be simple on W^r and our proposition is thereby proved.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Andreotti, "Recherches sur les surfaces algébriques irregulières," *Academie Royale de Belgique. Classes des Sciences. Mémoires. Collection in* 8°27, no. 7 (1952).

[2] W. L. Chow, "Abelian varieties over function fields," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 253-257.

[3] Y. Nakai, "Note on the intersection of an algebraic variety with the generic hyperplane," *Memoire of the College of Science, Kyoto University*, Ser. A, vol. 26 (1951), pp. 185-187.

[4] T. Matsusaka, "Polarized varieties, fields of moduli and generalized Kummer varieties of polarized Abelian varieties," *American Journal of Mathematics*, vol. 80 (1958), pp. 45-82.

[5] R. Torelli, "Sulle varietà di Jacobi," *Rendiconti della Reale Accademia dei Lincei*, serie 5ª, vol. 22 (1913), pp. 98-103.

[6] A. Weil, "Foundations of Algebraic Geometry," *American Mathematical Society Colloquium Publications*, vol. 29 (1946).

[7] ———, "Variétés Abéliennes et Courbes Algébriques," *Actualités Scientifiques et Industrielles*, No. 1064 (1948).

[8] ———, "Projective embeddings of Abelian varieties," *Algebraic Geometry and Topology* (A symposium in honor of S. Lefschetz), Princeton Mathematical series, pp. 177-181.

[9] ———, "On the theory of complex multiplication," *Proceedings of the International symposium on Algebraic Number Theory* (1955), pp. 9-22.

[10] ———, "Zum Beweis des Torellischen Satzes," *Nachrichten der Akademie der Wissenschaften in Göttingen.* Mathematisch-Physikalische Klasse, Nr. 2 (1957), pp. 33-53.

[11] O. Zariski, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques Severi," *Annals of Mathematics*, vol. 55 (1952), pp. 552-592.

ON THE PREPARATION OF MANUSCRIPTS.

The following instructions are suggested or dictated by the necessities of the technical production of the American Journal of Mathematics. Authors are urged to comply with these instructions, which have been prepared in their interests.

Manuscripts not complying with the standards usually have to be returned to the authors for typographic explanation or revisions and the resulting delay often necessitates the deferment of the publication of the paper to a later issue of the Journal.

Horizontal fraction signs should be avoided. Instead of them use either solidus signs / or negative exponents.

Neither a solidus nor a negative exponent is needed in the symbols $\frac{1}{2}$, $\frac{1}{\pi}$, $\frac{1}{2\pi}$, $\frac{1}{2\pi i}$, which are available in regular size type.

Binomial coefficients should be denoted by C_k^n and not by parentheses. Correspondingly, for symbols of the type of a quadratic residue character the use of some non-vertical arrangement is usually imperative.

For square roots use either the exponent $\frac{1}{2}$ or the sign $\sqrt{}$ without the top line, as in $\sqrt{}-1$ or $\sqrt{(a+b)}$.

Replace $e^{(\ )}$ by exp( ) if the expression in the parenthesis is complicated.

By an appropriate choice of notations, avoid unnecessary displays.

Simple formulae, such as $A+iB=\frac{1}{2}C^*$ or $s_n=a_1+\cdots+a_n$, should not be displayed (unless they need a formula number).

Use $'$ or d/dx, possibly D, but preferably not a dot, in order to denote ordinary differentiation and, as far as possible, a subscript in order to denote partial differentiation (when the symbol ∂ cannot be avoided, it should be used as $\partial/\partial x$).

Commas between indices are usually superfluous and should be avoided if possible.

In a determinant use a notation which reduces it to the form $\det a_{ik}$.

Subscripts and superscripts cannot be printed in the same vertical column, hence the manuscript should be clear on whether a_i^k or $a^k{}_i$ is preferred. (Correspondingly, the limits of summation must not be typed *after* the Σ-sign, unless either Σ_1^m or $\Sigma^m{}_1$ is desired.) If a letter carrying a subscript has a prime, indicate whether x_i' or x'_i is desired.

Experience shows that a tilde or anything else *over* a letter is very unsatisfactory. Such symbols often drop out of the type after proof-reading and, when they do not, they usually appear uneven in print. For these reasons we advise against their use. This advice applies also to a bar over a Greek or German letter (for the symbol of complex conjugation an asterisk is often allowed by the context). Type carrying bars over ordinary size italic letters of the Latin alphabet is available.

Bars reaching over several letters should in any case be avoided (in particular, type lim sup and lim inf instead of lim with upper and lower bars).

Repeated subscripts and superscripts should be used only when they cannot be avoided, since the index of the principal index usually appears about as large as the principal index. Bars and other devices *over* indices cannot be supplied. On the other hand, an asterisk or a prime (to be printed *after* the subscript) is possible on a subscript. The same holds true for superscripts.

Distinguish carefully between l. c. "oh," cap. "oh" and zero. One way of distinguishing them is by underlining one or two of them in different colors and explaining the meaning of the colors.

Distinguish between ϵ (epsilon) and $\in$ or ε (symbol), between x (eks) and $\times$ (multiplication sign), between l. c. and cap. phi, between l. c. and cap. psi, between l. c. k and kappa and between "ell" and "one" (for the latter, use $\mathfrak{k}$ and 1 respectively).

Avoid unnecessary footnotes. For instance, references can be incorporated into the text (parenthetically, when necessary) by quoting the number in the bibliographic list, which appear at the end of the paper. Thus: "[3], pp. 261-266."

Except when informality in referring to papers or books is called for by the context, the following form is preferred:

[3] O. K. Blank, "Zur Theorie des Untermengenraumes der abstrakten Leermenge," *Bulletin de la Societé Philharmonique de Zanzibar*, vol. 26 (1891), pp. 242-270.

In any case, the references should be precise, unambiguous and intelligible.

Usually sections numbers and section titles are printed in bold face, the titles "Theorem," "Lemma" and "Corollary" are in caps and small caps, "Proof," "Remark" and "Definition" are in italics. This (or a corresponding preference) should be marked in the manuscript. Use a period, and *not* a colon, after the titles Theorem, Lemma, etc.

German, script and bold face letters should be underlined in various colors and the meaning of the colors should be explained. The same device is needed for Greek letters if there is a chance of ambiguity. In general, mark all cap. Greek letters.

All instructions and explanations for the printer can conveniently be collected on a separate sheet, to be attached to the manuscript.

In case of doubt, recent issues of the Journal may be consulted.

American Journal of Hygiene. Edited by D. BODIAN, Managing Editor, A. M. BAETJER, R. M. HERRIOTT, F. B. BANG, P. E. SARTWELL, and T. B. TURNER. Publishing two volumes of three numbers each year, volume 65 is now in progress. Subscription $12 per year. (Foreign postage, 50 cents; Canadian postage, 25 cents.)

American Journal of Mathematics. Edited by W. L. CHOW, J. A. DIEUDONNÉ, A. M. GLEASON and PHILIP HARTMAN. Quarterly. Volume 80 in progress. $8.50 per year. (Foreign postage, 50 cents; Canadian, 25 cents.)

American Journal of Philology. Edited by H. T. ROWELL, LUDWIG EDELSTEIN, JAMES W. POULTNEY, JOHN H. YOUNG, JAMES H. OLIVER, and EVELYN H. CLIFT, Secretary. Volume 78 is in progress. $6.00 per year. (Foreign postage, 50 cents; Canadian 25 cents.)

Bulletin of the History of Medicine. OWSEI TEMKIN, Editor. Bi-monthly. Volume 31 in progress. Subscription $6 per year. (Foreign postage, 50 cents; Canadian 25 cents.)

Bulletin of the Johns Hopkins Hospital. E. K. MARSHALL, JR., Managing Editor. Monthly. Subscription $10.00 per year. Vol. 100 is in progress. (Foreign postage, 50 cents; Canadian, 25 cents.)

ELH. A Journal of English Literary History. Edited by E. T. NORRIS (Managing Editor) and D. C. ALLEN, G. E. BENTLEY, JACKSON I. COPE, RICHARD HAMILTON GREEN, J. HILLIS MILLER, ROY H. PEARCE, and E. R. WASSERMAN. Quarterly Volume 23 in progress. $4.00 per year. (Foreign postage, 40 cents; Canadian, 20 cents.)

Johns Hopkins Studies in Romance Literatures and Languages. †H. C. LANCASTER, Editor. Seventy-six numbers have been published.

Johns Hopkins University Studies in Archaeology. DAVID M. ROBINSON, Editor. Thirty-nine volumes have appeared.

Johns Hopkins University Studies in Geology. JOSEPH T. SINGEWALD, JR., Editor. Sixteen numbers have been published.

Johns Hopkins University Studies in Historical and Political Science. Under the direction of the Departments of History, Political Economy and Political Science. Volume 75 in progress.

Modern Language Notes. NATHAN EDELMAN, General Editor. Eight times yearly. Volume 72 in progress. $6 per year. (Foreign postage, 50 cents; Canadian, 25 cents.)

A complete list of publications will be sent on request

There was published in 1956 a 64-page

INDEX

to volumes 51-75 (1929-1953) of

THE AMERICAN JOURNAL OF MATHEMATICS

The price is $2.50. A 60-page Index to volumes 1-50 (1879-1928), published in 1932, is also available. The price is $3.00.

Copies may be ordered from The Johns Hopkins Press, Baltimore 18, Maryland.